数学名著译丛

普林斯顿数学指南

（第一卷）

〔英〕Timothy Gowers 主编

齐民友 译

科学出版社

(O-5356.01)

数学名著译丛

拓扑空间论
代数特征值问题
数学概观
常微分方程
数学与猜想
代数几何
数学 —— 它的内容，方法和意义
微积分和数学分析引论
代数数理论讲义
非线性及泛函分析 —— 数学分析中的非线性问题讲义
数学的发现 —— 对解题的理解、研究和讲授
代数拓扑基础
博大精深的素数
环与模范畴
代数几何引论
代数学 I
代数学 II
控制论(或关于在动物和机器中控制和通信的科学)(第二版)
微分几何基础 (第一卷)
一般拓扑学
能量分析攻击
线性算子理论
数学物理方法 I
数学物理方法 II
流形上的分析
普林斯顿数学指南(第一卷)
普林斯顿数学指南(第二卷)
普林斯顿数学指南(第三卷)

www.sciencep.com



科学数理分社
电 话：(010) 64033664
E-mail：math-phy@mail.sciencep.com
网 址：http://www.math-phy.cn

销售分类建议：高等数学

定 价：128.00 元

数学名著译丛

普林斯顿数学指南

第一卷

［英］Timothy Gowers　主编

齐民友　译



科学出版社

北　京



图字：01-2013-6961 号

内 容 简 介

本书是由 Fields 奖得主 T. Gowers 主编、133 位著名数学家共同参与撰写的大型文集. 全书由 288 篇长篇论文和短篇条目构成, 目的是对 20 世纪最后一二十年纯粹数学的发展给出一个概览, 以帮助青年数学家学习和研究其最活跃的部分, 这些论文和条目都可以独立阅读. 原书有八个部分, 除第Ⅰ部分是一个简短的引论、第Ⅷ部分是全书的“终曲”以外, 全书分为三大板块, 核心是第Ⅳ部分“数学的各个分支”, 共 26 篇长文, 介绍了 20 世纪最后一二十年纯粹数学研究中最重要的成果和最活跃的领域, 第Ⅲ部分“数学概念”和第Ⅴ部分“定理与问题”都是为它服务的短条目. 第二个板块是数学的历史, 由第Ⅱ部分“现代数学的起源”(共 7 篇长文)和第Ⅵ部分“数学家传记”(96 位数学家的短篇传记)组成. 第三个板块是数学的应用, 即第Ⅶ部分“数学的影响”(14 篇长文章). 作为全书“终曲”的第Ⅷ部分“结束语：一些看法”则是对青年数学家的建议等 7 篇文章.

中译本分为三卷, 第一卷包括第Ⅰ~Ⅲ部分, 第二卷即第Ⅳ部分, 第三卷包括第Ⅴ~Ⅷ部分.

本书适合于高等院校本科生、研究生、教师和研究人员学习和参考. 虽然主要是为了数学专业的师生写的, 但是, 具有大学数学基础知识, 更重要的是对数学有兴趣的读者, 都可以从本书得到很大的收获.

图书在版编目(CIP)数据

普林斯顿数学指南. 第 1 卷/(英)高尔斯(Gowers, T.)主编；齐民友译. —北京：科学出版社, 2014.1
(数学名著译丛)
书名原文：The Princeton Companion to Mathematics
ISBN 978-7-03-039321-0
Ⅰ.①普… Ⅱ.①高… ②齐… Ⅲ.①数学-高等学校-教学参考资料 Ⅳ.①O1
中国版本图书馆 CIP 数据核字(2013) 第 297983 号

责任编辑：赵彦超 / 责任校对：桂伟利
责任印制：赵德静 / 封面设计：陈 敬

科学出版社 出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com

骏杰印刷厂 印刷
科学出版社发行 各地新华书店经销
*
2014 年 1 月第 一 版 开本：720 × 1000 1/16
2014 年 1 月第一次印刷 印张：33 1/2
字数：748 000

定价：128.00 元

(如有印装质量问题，我社负责调换)

译者序

我有幸接触到《普林斯顿数学指南》(以下简称《数学指南》) 这部书并且开始翻译工作是 2010 年的事了, 到读者能够见到它, 就有五个年头了. 这四年的经历可以说是好比重进了一次数学系, 不过与第一次进数学系比较, 真正的差别不在于自己的数学准备比当年要高一些, 所学的科目内容比当年更深了, 而是我必须认真地逐字逐句读完这本 "教科书". 当我上一次进数学系时, 所学的课程内容离当时 (20 世纪 50 年代) 还很少有少于 100 年的时间间距, 而这一次所学的内容则主要是近一二十年的事情. 时间间距一长就有一个好处: 后人可以更好地整理、消化这些内容, 对于许多问题也就可以了解得更真切. 而如果在上次进数学系时, 想要学习当时正在发展中的数学, 如果没有比较足够的准备, 不曾读过一些很艰深的专著和论文, 就常会有不知所云如坠云雾中的感觉. 但是这一次 "再进数学系" 的感觉就不太相同了, 一方面, 对于自己原来觉得已经懂了, 甚至后来给学生们讲过多次的内容, 现在发现并没有真懂. 还是用前面用的 "真切" 二字比较恰当: 当年学到的东西还是表面的、文字上的更多一些, 而对于当时人们遇到的究竟是什么问题, 其要害何在, 某一位数学家的贡献何在, 甚至为什么说某位数学家伟大, 自己都是糊里糊涂, 所以说是懂得并不 "真切", 而这一次有了比较深刻的感觉. 另一方面, 我必须要学习一些过去不曾读过的甚至没有听到过的课程, 就本书的核心 —— 第Ⅳ部分: 数学的各个分支 —— 而言, 其中一些篇章我只能说是 "认得其中的字", 对其内容不能置一词. 但是对于多数篇章, 感觉与读一本专著 —— 哪怕是这个分支的名著 —— 比较, 就有一种鸟瞰的感觉了: 它们没有按我们习惯的从最基本的定义与最基本的命题开始, 而是从数学发展在某个时代遇见的某个问题开始 (这本书有篇幅很大的关于历史和数学家传记的部分, 对于理解各个分支的实质很有帮助), 讲述当时的数学家是怎样对待这些问题的, 他们的思想比前人有何创新, 与后世比又有哪些局限. 这些文章还讲这个分支为什么以那些工作为核心, 与其他的工作有什么关系. 这些文章一般都以 "谈话" 的形式呈现在读者面前, 使您感到作者是娓娓道来, 吸引着听众, 这可能是使得此书能吸引人而不令人感到枯燥的原因之一. 不过, 读者对于一本书有什么样的要求, 对它的观感和应该采用的读法是不同的. 如果只是为了扩大眼界, 那是一种读法; 如果是为了听懂同行的讲演讲的是什么东西, 甚至自己也能提出相关的问题, 那就是另一种读法了. 更重要的是, 如果读者认为某一个分支引起了他的兴趣, 因而有了进一步了解它的愿望 —— 这正是原书编者希望达到的目的 —— 那就需要对于书中（或某一篇章中）提到的某个问题有进一

步的知识. 原书编者多次提到《数学指南》这本书与一些大型数学网站的不同, 但我认为, 为了进一步了解这个问题, 把《数学指南》与一些大型数学网站的相关条目结合起来读不失为有效的办法, 特别是维基百科, 在翻译过程中给了我很大的帮助, 不仅使我能更准确地了解此书某一篇章, 甚至是某一段落的含义, 少犯太离谱的错误, 而且更重要的是当我想要进一步了解一些问题时, 这些网站给了我很大的帮助. 相信对于读者也会是这样, 所以译者有时在脚注中特别介绍了所用到的网站. 不过在脚注中提到一些网站只占实际用到它们的频度的很小一部分.《数学指南》还有一个可能读者没有想到的用处: 近年来, 关于数学的新进展, 特别是一些新的应用, 圈子内外常有一些似是而非的流言, 而且常在大学生中传播, 在多数情况下,《数学指南》会提供比较可靠的说明.

最重要的是要强调一下, 学数学是要下力气的, 而要想真正学到一点东西, 认真地读一些教科书、专著, 特别是名著是不可少的. 译者愿意特别向年轻的读者提醒一下,《数学指南》(或者书的原名 "Companion", 直译就是 "伴侣") 只能给您指一条路, 陪您走上一段, 它不可能让您毫不费力就懂一门数学, 那种不需要费力就能学有所成 (当前特别指能金榜题名), 不只是似是而非的流言, 老实说就是不负责任的谎言.《数学指南》的作用是使我们花的功夫能花在关键处, 起较大的作用.

这一段话对于读者和译者都是适用的. 这本译作, 可以看成是译者 "再进数学系" 的考卷. 这样一本千余页的大作, 其内容又有很大一部分是我所不熟悉, 或者完全不懂的, 翻译的错误在所难免, 还是反映了翻译时下的功夫不够. 如果读者愿意赐教, 就是帮助译者更好地 "上这一次数学系", 所以译者在此预先致以诚挚的谢意.

这本书还有一个篇幅不大的引论部分, 由四篇文章组成. 其中第二和第三两篇分别讲 "数学的语言和语法" 和 "一些基本的数学定义". 第二篇包含了对于逻辑学的简单介绍, 第三篇则分门别类对数学的各个分支 (如代数、几何、分析等) 的基本概念作一些说明. 按编者原来的意图, 如果对于这些材料太过生疏, 读这本书就会很困难. 问题在于即使知道了这些, 是否就能比较顺利地读这本书? 按译者的体验, 大概还是不行的, 因为这两篇文章有点类似于名词解释, 其深度与其他各部分特别是与作为本书主体的第Ⅳ部分 "数学的各个分支" 反差太大. 依译者之见, 不妨认为这一部分是对于读者的要求的一个大纲. 对这一部分 (或者例如对于其中的分析部分) 有了一个大学本科的水平, 再读本书 (有关分析的各个篇目) 就方便多了 (当然, 如上面说的那样, 许多时候还需要再读一点进一步的书). 这样, 不妨认为原书在这里提出: 为了涉猎现代数学, 读者需要懂得些什么, 或者说, 大学数学专业应该教给学生的是什么? 如果大家不反对这个想法, 则回过头来看一下现在国内的大学数学教学, 就会承认还需要走相当一段路程, 因此建议本书的读者先读一下这两篇文章, 那么下面应该读些什么就清楚了.

最后, 关于译文的文字还有几句需要说的话. 我们大家都有一个体会: 同是一件事, 如果多说一句甚至半句话就会清楚多了, 写数学书当然也是一样, 但是这就涉及作者的素养和习惯了. 也许对作者来讲, 话已经讲够了, 而对译者就需要好好揣摩这里少讲的这一句甚至半句话. 这些话译者原来打算就放在一个方括号内, 但是后来这种情况多了, 译者又常把这个方括号略去, 使版面更清楚一些, 而只在加的话比较多的时候加以说明. 这样, 译文与原书就有了一些区别. 此外原书有一些笔误或排版的错误, 译者就改了算了, 但是涉及内容的, 译者都加了说明, 以示文责自负.

最后, 再说一次, 请读者赐教并指出翻译的错误, 谨致诚挚的谢意.

齐民友

2013 年国庆日

序

1. 这是一本什么书

罗素 (Bertrand Russell) 在他所写的《数学原理》(*The Principle of Mathematics*) 中给出了纯粹数学的以下定义：

> *纯粹数学就是所有形如"p 蕴含 q"的命题的集合，这里 p 和 q 是含有相同的一个或多个变项的命题，而且除逻辑常项以外不含其他常项. 这些逻辑常项全都可以用下述概念来定义：蕴含、项对于类的"为其元素"的关系、使得的概念*[①]*、关系的概念，以及上述形式命题的一般概念中可能包含的其他概念. 除此以外，数学还使用一个概念，但它不是其所考虑的命题的成分，这就是真理的概念.*

《普林斯顿数学指南》可以说是罗素的定义所没有包含的一切东西的全讲.

罗素的《数学原理》是 1903 年出版的，当时有许多数学家全神贯注地研究这门学科的逻辑基础. 现在，一个多世纪已经过去了，如罗素所描述的那样，把数学看作一个形式系统，这一点现在也不再是一个新思想，而今天的数学家更关心的是别的事. 特别是在有这么多数学结果问世的这样一个时代，每个人只可能懂得其中极小的一部分；只知道哪些符号排列构成语法上正确的数学命题已经不那么有用，更需要知道的是哪些命题才值得注意.

当然，不能希望对于哪些命题值得关注这个问题给出完全客观的回答，不同的数学家对于哪些东西才有意思会有不同意见也是合乎情理的. 所以，这本书远不如罗素的书那么形式化，它的许多作者各有不同的观点. 这样，本书并不试图对于"是什么使得一个数学命题有意思"给出准确的答案，而是只想向读者提供一些很大的具有代表性的例子，使他们知道数学家们在 21 世纪开始的时候为之拼搏的思想是什么，并且以尽可能吸引人及能够接受的方式来做这件事.

2. 本书的范围

本书的中心点是现代纯粹数学，关于这个决定有几句话要说. "现代"一词如上面所说，只不过是说本书打算对于现在数学家们在做什么给出一个概念. 举例来

---

① 请参看 I.2 §2.1"集合"这一小节第三段中对"使得"这一概念的解释.—— 中译本注

说, 一个领域可能在 20 世纪中叶发展比较迅速, 现在达到了一个比较固定的形式, 那么人们对它的讨论比之对现在快速发展中的领域就会少一些. 然而, 数学是有历史的: 要理解一点现代的数学, 通常就需要知道许多早就发现了的观念和结果. 此外, 想要对于今天的数学有一个恰当的展望, 知道一点它何以成了今天的情况就是很必要的了. 所以在本书里讲了大量的历史, 尽管把这些历史包括进来的主要原因是为了说明今天的数学.

"纯粹" 一词就更麻烦一些. 许多人曾经评论过, 在纯粹与应用数学之间并没有清楚的分界线, 而且正如对现代数学要有一个适当的理解, 就需要一点其历史的知识一样. 对纯粹数学要有一个适当的理解, 就需要一点应用数学和理论物理的知识. 说真的, 这些领域曾经为纯粹数学提供了许多基本的观念, 而由之产生了纯粹数学的许多最有趣、最重要、当前又最活跃的分支. 本书对于这些其他分支对纯粹数学的影响肯定不能视而不见, 也不能忽视纯粹数学的实际和心智的应用. 然而, 本书的范围比它应该的那样要更加狭窄一些. 有一个阶段, 打算为本书起一个比较准确的书名, 叫做 "普林斯顿纯粹数学指南", 不采用它的唯一原因是觉得现在的书名更好一些.

类似这本集中于纯粹数学这样一个决定后面还有一个想法, 就是它会为以后再出一本 "指南" —— 关于应用数学和理论物理的 "指南" 留下余地. 在这样一本书尚未出现以前, Roger Penrose 所写的《通向现实的道路》(*The Road to Reality*)(New York: Knopf, 2005) 一书包含了数学物理学的很广泛的论题, 而且是按照与本书很相近的水平写的, Elsevier 最近也推出了五卷本的《数学物理学百科全书》(*Encyclopedia of Mathematical Physics*)(Amsterdam: Elsevier, 2006).

3. 这不是一部百科全书

"指南" 这个词很值得注意. 虽然本书肯定是打算写成一本有用的参考书, 您可不能对它期望过高. 如果您想找出一个特定的数学概念, 就不一定能在这里找得到, 哪怕它是一个重要的概念, 虽然说, 如果它越重要, 就越有可能被收入本书. 在这一方面, 这本书倒有点像是真有一个人对读者在作 "指南": 这个人在知识上有漏洞, 对于某些主题在看法上又不一定与众人相同. 虽然声明了这一点, 我们至少还是力求某种平衡: 许多主题并未包括在书中, 但是已经收入的范围还是很广泛的 (比起您对真有其人作 "指南" 所能合理希望的、要广泛得多). 为了达到这种平衡, 我们在某种程度上是以一些 "客观的" 指标为导引的, 例如美国数学会的数学主题的分类, 或者四年一届的国际数学家大会上对数学分类的方法. 大的领域如数论、代数、分析、几何学、组合学、逻辑、概率论、理论计算机科学和数学物理, 本书都是有的, 但是它们的各个子分支就不一定都有了. 关于选择哪一些主题收入本书, 每一

个主题要写多长, 不可避免地并非某个编辑的规定所能决定的, 而是取决于某些高度偶然的因素, 例如谁愿意写, 在同意写以后是谁实际交了稿, 交来的稿子是否符合规定的字数等等. 结果, 有些领域反映得不如我们所希望的那么充分. 终于到了这样一个关节点: 印行一部不甚完备的书, 比之为了达到完美的平衡而再等上几年还要好些. 我们希望有朝一日《普林斯顿数学指南》(以下简称《数学指南》) 还会有新版, 那时就可以弥补本版可能有的缺陷了.

另外一个方面, 本书也不同于一部百科全书, 即本书是按主题排列, 而不是按字母顺序排列的. 这样做的好处是, 虽然各个条目可以分开来阅读, 却也可以看作是一个和谐的整体的一部分. 说真的, 这本书的结构是这样的, 如果从头到尾地读, 虽然会花费太多时间, 却也不是好笑的事情.

4. 本书的结构

说本书是 "按主题排列的", 这是什么意思? 回答是: 本书分成了八个部分, 各有其总的主题和不同的目的. 第 I 部分是引论性质的材料, 对数学给出一个总的鸟瞰, 并且为了帮助数学背景较浅的读者, 解释了这个学科的一些基本的概念. 一个粗略的来自经验的规则是: 如果一个主题属于所有数学家必备的背景, 而不是特定领域的数学家之所需, 就把它纳入第 I 部分. 举两个明显的例子: *群*[I.3§2.1] 和*向量空间*[I.3 §2.3] 就属于这个范畴.

第II部分是一组历史性质的论文, 目的是解释现代数学的极具特色的风格是怎样来的. 广泛地说, 就是解释现代的数学家在其学科中的思维方式与 200 年前 (或者更早) 的数学家的思维方式有哪些主要的区别. 有一点区别在于, 对于什么算是证明, 现代有了大家都能接受的标准. 与此密切相关的是这样一件事实, 即数学分析 (微积分及其后来的扩张和发展) 已经被放置在严格的基础上了. 其他值得注意的特点还有数的概念的扩张、代数的抽象性, 另外, 绝大多数现代几何学家研究的是非欧几何, 而不是更加熟悉的三角形、圆、平行线之类.

第 III 部分由一些较短的条目组成, 每一条讨论一个在第 I 部分中未曾出现的重要的数学概念. 目的是: 如果有一个您不知道但又时常听人说起的概念, 本书这一部分就是一个查找的好地方. 如果另一位数学家, 比方说一位讲演的人, 假定您熟悉一个定义 —— 例如*辛流形*[III.88], 或者*不可压缩流欧拉方程*[III.23], 或者*索伯列夫空间*[III.29 §2.4], 或者*理想类群*[IV.1 §7]—— 要承认自己不懂又感到没面子, 现在您就有了一个脱身的办法: 在《数学指南》里面查一查这个定义.

第 III 部分的文章如果只是给出一些形式定义, 那就没有什么用处: 要想懂得一个概念, 人们总会希望知道它直观地是什么意思, 它为什么重要, 而第一次引入它是为的什么. 特别是如果它是一个相当广泛的概念, 人们就会想知道一些好的例

子 —— 既不太简单, 又不太复杂. 事实上, 很可能提出并且讨论一个选择得很好的例子, 正是这篇文章需要做的事情, 因为一个好例子比一个一般定义好懂得多, 而一个比较有经验的读者能够从抽取这个例子里面重要的性质来写出一般定义.

第 III 部分的另一个作用是为本书的心脏部分 (即第 IV 部分) 提供支持. 第 IV 部分是关于数学的不同领域的 26 篇文章, 它们比第 III 部分的文章要长得多. 第IV部分的每一篇典型的文章都是为解释它所讨论的领域的某些中心思想和重要结果, 而且要做得尽可能不太形式化, 又得服从一个限制, 就是不能太模糊, 以至不能提供信息. 对于这些文章, 原来的希望是写成 "床头读物", 就是既清楚又很初等, 不必时而停下来思考就能读懂它们. 所以在选择作者的时候, 有两个同等重要的优先条件: 专业水平和讲解的本事. 但是, 数学不是一门容易的学科, 所以到了最后, 我们只好把原来定的完全可接受性看成是一个要为之努力的理想, 尽管在每一篇文章的最小的小节里未能完全达到. 但是, 哪怕这篇文章很难读, 它的讨论比起典型的教科书来也会更清楚, 更少形式化, 这一点时常做得相当成功. 和第 III 部分一样, 好几位作者是通过观察有启发性的例子来做到这一点的, 例子后面有的接着讲更一般的理论, 有的则让例子本身说话.

第 IV 部分有许多文章包含了对于数学概念出色的描述, 这些概念本来应该放到第III部分用专文讲解的. 我们本想完全避免重复, 而在第 III 部分里交叉引用这些描述. 但是, 这会让读者不高兴, 所以采用了下面的两全之策: 如果一个概念已经在别处充分地解释了, 而第 III 部分又没有设专文, 就做一个简短的描述再加上交叉引述. 这样一来, 如果您想很快地看一看一个概念, 就可以只看第 III 部分, 如果需要更多细节, 就得跟着引文看本书的其他部分了.

第 V 部分是第 III 部分的补充, 它也是由重要数学主题的短文组成的, 但是现在这些主题是数学中的一些定理和未解决的问题, 而不是基本对象和研究工具. 和全书一样, 第 V 部分里条目的选择必定远非全面, 而是在心目中有一些准则. 最显然的一个准则是它们在数学中的重要性, 但是有些条目的选择是因为可以用一种使人愉快的又容易接受的方式来讨论它们, 还有一些是因为它们有不平常的特殊之处 (**四色定理**[V.12] 是一个例子, 虽然说按照别的准则, 也可能会选入这一条), 有一些条目是因为第IV部分的密切相关条目的作者觉得有一些定理应该单独讨论, 还有一些是因为有几篇文章的作者需要它作为背景知识. 和在第 III 部分一样, 第 V 部分有一些条目不是完整的文章, 而是简短的说明加上交叉引用.

第VI部分是另一个历史部分, 是关于著名数学家的. 它由一些短文组成, 每一篇的目的是给出一些很基本的传记资料 (例如国籍和生卒年月), 并且说明这位入选的数学家何以是著名的数学家. 一开始, 我们计划把在世的数学家也包括在内, 但最后我们得出了一个结论, 对于今天仍然在工作的数学家, 几乎不可能做一个令人满意的选择, 所以我们决定限于已经去世而且主要是由于 1950 年以前的工作而

著称的数学家. 比较晚近的数学家因为在另外的条目里也会提到, 当然也就进入本书了. 对他们没有专门列条目, 但是在索引里看一看, 就会对他们的成就有个印象了.

在主要关于纯粹数学的六个部分以后, 第 VII 部分最终展示了数学从外界得到的实用上和心智上的推动. 这部分里面是一些较长的文章, 有一些是由具有跨学科兴趣的数学家写的, 有些则是由使用了很多数学的其他学科专家写的.

本书的最后一部分包含了对于数学的本性和数学生活的一般的反思. 这一部分里的文章, 比前面较长的文章, 总体上说要好读一些, 所以尽管第VIII部分是本书的结尾, 有些读者也可能从它们开始来读本书.

各部分里面文章的次序, 在第III部分和第 V 部分是按字母顺序排列的, 而第VI部分则按年代排列. 按生卒年月来安排数学家传记, 这个决定是经过了仔细考虑的. 这样做有几个理由: 它会鼓励读者从头到尾地读, 而不是选择单篇地读, 以获得对于这门学科的历史感; 它会使得读者对于哪些数学家是同时代人或者近乎同时代人, 要清楚得多. 如果读者费一点心, 在考察一位数学家的时候, 猜想一下他 (或者她) 的出生年月和其他数学家的出生年月相对关系如何, 就会得到一点虽然很小但又很有价值的知识.

在其他部分内部, 做了一些努力来按照主题排列这些文章. 特别是在第IV部分里, 希望次序的排列符合两个基本原则: 首先, 关系密切相关的分支的文章要尽量靠近; 其次, 如果在读文 B 之前先读文 A 有明显的意义, 那么在本书里就把文 A 放在文 B 前面. 这件事说起来容易做起来难, 因为有些分支很难分类, 举一个例子, 算术几何是算代数、几何还是算数论呢? 分在这三类都有道理, 决定采用其一总是有点造作. 所以第IV部分里的次序并不是分类的一种格式, 而只是我们能够想到的最佳的线性次序.

至于各个部分次序的排列, 则目的在于使之成为从数学观点看来最自然的次序, 并且给本书一种方向的感觉. 第 I , II 两部分显然是导引性质的. 第III部分放在第IV部分前面, 是因为想要了解一个领域, 就总要先和新定义格斗一番. 但是第IV部分放在第 V 部分前面, 则是因为为了领会一个定理, 先知道它在一个领域里面的位置如何, 这是一个好主意. 第VI部分放在第III部分到第 V 部分后面, 是因为知道一点数学以后, 才能更好地领会一位著名数学家的贡献. 第VII部分接近书末, 也是由于类似的理由: 要理解数学的影响, 先得理解数学. 第VIII部分的反思带有结束语的意思, 是离开这本书的适当的时候.

5. 交叉引用

从一开始,《数学指南》这本书就计划要有大量的交叉引用 (即在书内引用本书

内另外地方). 在这篇序里面就已经有了一两次交叉引用了, 而这种情况我们用楷体来表示. 例如引用辛流形[III.88], 就表示辛流形将在第III部分的第 88 个条目里讨论, 而引用理想类群[IV.1 §7], 则把读者带到第IV部分的第一个条目的 §7(总之, 交叉引用的数字首先是一个罗马数字, 表示哪一部分, 紧接着的一个阿拉伯数字则表示哪一个条目, 而文字就是这个条目的标题, 或条目内的相关内容. 每一条目分成若干节, 引用时就需要标明节号, 例如 [IV.1 §7] 就表示进入这一条目后的第 7 节, 节下面有小节 (subsection) 和小小节 (subsubsection), 这就用逗号表示. 标题中的文字就是这一节或小节的标题或其中的内容. 在正文中, 条目的标题放在双线里面 (中译本没有双线), 而节与小节的标题则放在正文内节或小节的起始处, 记号 § 则不再出现. 在小小节以下有时还有 "小小小节"(subsubsubsection), 所以还会出现 §3.1.2 这样的记号).

我们尽了最大努力来编写一本读起来很愉快的书, 而交叉引用的目的也是希望有助于使读者愉快. 说来也怪, 因为在读书时要中途打断, 花上几秒钟去查阅书中其他地方, 本来会使人感到麻烦. 然而, 我们也试图使得每一篇文章读起来可以不必查找他处. 这样, 如果您不想追随这种交叉引用, 那么通常也可以不这么做. 重要的例外在于对各位作者, 曾经允许他们假设读者对于第 I 部分里讨论的概念有一些知识. 如果您全然没读过大学水平的数学课程, 我们建议您全文读一下第 I 部分, 这会大为减少读以下的条目时再到他处搜寻的必要.

有时一个概念是在一个条目里介绍的, 而又在同一条目里解释. 在数学文章里这时通用的规约是在定义这个词时, 用斜体来印这个词. 我们也想遵从这个规约, 但是在如本书条目这种非正式的文章里, 要想说清楚何时算是在定义一个新的或不熟悉的名词, 并不总是很清楚 (再说, 中译本里, 楷体还有其他用处), 所以本书采用了一个粗略的规定：凡是第一次见到一个词, 而且紧接着就对它进行解释, 这时就用黑体排印这个词. 对一些以后并未作解释的词, 有时我们也使用了黑体*, 表示为了懂得下面的条目, 并不需要懂得这个词. 在更极端的情况下, 则使用双引号来代替黑体.

许多条目结尾处都有一个 "进一步阅读的文献" 的一节, 它们其实是对于进一步阅读的建议, 不要把它们看作是通常的综述文章后面所列的那种完整的参考文献. 与此相关的还有以下的事实：《数学指南》主要关心的不在于对发现所讨论主题的数学家记述其功绩, 也不在于引述这些发现出处的文章. 对于这些原始根源有兴趣的读者, 在建议进一步阅读的书或文章里面或在因特网上可以找到这些资料.

---

* 在翻译此书时, 我们有时也遵照其他数学文献的习惯, 把重要的概念、名词等用黑体排印. —— 中译本注

6. 本书是针对谁编写的

原来的计划是要求《数学指南》的全书对于任何具有良好的高中数学背景 (包括微积分) 的读者都是能接受的. 然而, 很快就变得很明显, 这是一个不可能实现的目标: 有一些数学分支, 对于至少知道一点大学水平数学的人来说就非常容易, 而企图向水平更低的人们来解释, 就没有什么道理了. 另一方面, 这个学科也有一些部分, 肯定能够对于没有这个额外经验的读者解释清楚. 所以, 我们最后放弃了这本书应该有一个统一的难度水平的想法.

然而, 可接受性仍然是我们最优先的考虑. 在全书里, 我们都力求在实际上可以做到在最低水平上来讨论数学思想. 特别是编者们用了很大的力气, 避免任何自己不懂的材料进入本书, 而这一点成了一个很严重的限制. 有些读者会觉得一些条目太难, 而另一些读者又会觉得另一些条目太容易, 但是我们希望所有具有高中以上水平的读者都能享受本书的很实在的一大部分.

不同层次的读者都能够从《数学指南》中得到些什么? 如果您已经着手在读一门大学数学课程, 就会觉得这门课程给您提出了许多困难而又不熟悉的材料, 而您对于它们何以重要, 又引向何方, 则不甚了然. 这时, 使用《数学指南》就可以为您提供关于这个主题的一些展望 (举一个例子, 知道什么是环的人的数目, 比能够说明为什么要关注环的人的数目要多得多, 本书的条目环, 理想与模 [Ⅲ.81]和代数数[Ⅳ.1] 就会告诉您关注环的理由是什么).

如果您读完了大学数学课程, 就可能会对做数学研究有了兴趣. 研究工作究竟是怎么回事? 大学本科课程, 在典型情况下, 极少能让您了解. 那么, 您怎么才能决定数学的哪一个领域在研究工作水平上确会使您有兴趣? 这件事并不容易, 但是您做的决定会产生极大区别: 要么您会幡然醒悟不搞数学了, 而博士学位也不要了, 要么您会继续在数学里走向成功的生涯. 这本书, 特别是第Ⅳ部分, 会告诉您, 不同类型的在研究工作水平上的数学家想的是什么, 从而可以帮助您在更加知情的基础上做出决定.

如果您已经是一个站住脚的数学家, 这本书对于您的主要用处可能是: 它将帮助您更好地理解您的同事们其实在做什么事情. 绝大多数非数学家, 当他们知道数学已经变得多么异乎寻常的专业化时, 都会非常吃惊. 近年来, 一个很好的数学家可能对于另一位数学家的论文完全看不懂, 哪怕二者的领域相当接近, 这并不是很罕见的事, 但这不是健康的状况. 做任何一件改善数学家之间的交流的事情都是一个好主意. 本书的编者们通过仔细阅读这些条目受益匪浅, 我们希望许多其他人也能获得同样的机会.

7. 本书提供了哪些因特网未能提供的东西

《数学指南》的特性在某些方面类似于那些大型的数学网站, 如维基百科的数学部分, 还有 Eric Weinstein 的 "Mathworld"(http://mathworld.wolfram.com/). 特别是交叉引用有一点超链接的味儿. 那么, 写这本书还有什么必要呢?

在目前, 答案是还有必要. 如果您曾经试过在因特网上查找一个数学概念, 就会知道这是一件碰运气的事. 有时候您会找到一个好的解释, 给出您正在寻找的信息. 但是, 时常则并不如此. 上面提到的那些网址肯定是有用的, 对于本书没有涵盖的材料, 我们也向您推荐在这些网址里去查找. 但是这些网上的文章与我们这里的条目, 写作的风格大不相同：网上的文章比较枯燥, 更加注重以更简洁的方法来给出基本事实, 而不是注重对这些事实的反思. 在网上也找不到如本书第 I, II, IV, VII和第VIII部分里面的那些长文章.

有人觉得把大量材料集中成书本的形式是有好处的. 但是, 我们在上面已经提到了, 本书并不是孤立的条目的简单汇集, 而是仔细排列了次序, 这样编纂出来的所有的书, 都必定有线条形的构造, 而这是网页所没有的. 一本书的物理性质又使得翻阅一本书和在网上漫游是完全不同的体验：读过了一本书的目录, 对于全书就能找到一点感觉; 而对于一个大的网站, 您只能对正在读的那一页有点感觉. 并不是每个人都同意这一点, 或者反而觉得这是书本形式的一个很值得注意的优点, 但是许多人无疑会觉得如此, 而本书就是为这些人编写的. 所以在目前《普林斯顿数学指南》还没有网上的对手, 本书不是想与现有的网站竞争, 而是想作为一个补充.

8. 本书的创意和团队[①]

编《普林斯顿数学指南》这样一本书的主意是 David Ireland 在 2002 年提出来的, 那时他在普林斯顿大学出版社的牛津办事处工作. 这本书的最重要的特点 —— 它的书名, 它如何由那些部分组成, 以及有一部分应该是关于数学的主要分支的条目 —— 这些都来自原来的想法. 他来到剑桥看望我, 讨论他的建议, 而到了"图穷匕首见"的时刻 (我知道会有这么一刻), 他要求我来编辑此书时, 我基本上是当场就接受了.

是什么促使我做出这个决定? 部分地是由于他告诉我, 并不希望我自己来做所有的事：不仅会有其他编者, 还会有相当的技术与行政的支持. 但是一个更基本的

① 原文标题是"How the companion came into being", 其内容是此书是怎样来策划, 以及主编团队的组成, 而未涉及具体的编辑工作. 中译本改成现在的标题是为了与下一节相区别.—— 中译本注

理由是, 写这本书的主意很像我自己做研究生时闲散时刻里有过的一个想法, 那时我想, 要是有什么地方能够找到一本写得很好的文集, 把数学不同领域里的大的研究主题都展示出来, 这该有多好. 这样, 一个小小的幻想就诞生了, 而突然之间我就有机会把它变成现实了.

我们从一开始就觉得, 这本书要包含相当多的历史思考, David Ireland 在我们见面以后很快就问 June Barrow-Green 是否准备担任另外一位编辑, 特别负责历史部分. 我们非常高兴, 她接受了, 而因为她的相当广泛的接触圈子, 我们或多或少地能够和全世界的数学史家有了来往.

然后又见了好几次面, 讨论书的内容, 结果就是向普林斯顿大学出版社提出正式建议. 出版社把这个建议发给一个专家顾问小组, 而虽然有几位专家指出了一个一定会提的问题, 就是这个计划大得惊人. 所有的人都对它很有热情. 下一阶段当我们开始寻找撰稿人的时候, 我们遇到的热情也很明显. 很多人对我们倍加鼓励, 说是很高兴这样一本书正在筹划之中, 也肯定了我们已经想到的事, 即市场上确实存在空缺. 在这个阶段, 我们很得益于《牛津音乐指南》的编者 Alison Latham 的建议与经验.

2003 年中, David Ireland 离开了普林斯顿大学出版社, 也带走了这几个计划. 这是一个大的打击, 我们惋惜没有了他对于这本书的远见与热情, 我们希望最终编出来的书仍然类似于他原来之所想. 然而, 大约在同时又有了正面的发展, 普林斯顿大学出版社雇佣了一家小公司: T&T Production Ltd, 它的责任是把撰稿人送来的文档编成一本书, 还要做许多大量的日常工作, 例如寄出合同, 提醒撰稿人交稿日期快到了, 接收文档, 对于已经做好的事情做记录等等, 绝大部分这类工作都是 Sam Clark 做的, 他在这方面的工作特别出色, 而且能奇迹般地保持好脾气. 此外在不需要许多数学知识的地方, 他还做了许多编辑工作 (尽管作为一位前化学家, 他比绝大多数人还是多懂得一点数学). 由于有 Sam 的帮助, 我们不仅有了一本细心编辑的书, 而且书的设计也很漂亮. 要是没有他, 我还真不知道这本书怎么能编撰出来.

我们继续举办正规的聚会, 更详细地计划这本书, 讨论其进展. 这些聚会都是由 Richard Baggaley 很能干地组织和主持的, Richard Baggaley 也是普林斯顿大学出版社牛津办事处的. 他一直这样做到 2004 年夏天由普林斯顿大学出版社的新的文献编辑 (reference editor)Anne Savarese 接手为止. Richard 和 Anne 都起了很大的作用, 而当我们忘记书的某些部分没有按计划进行时, 他们就会提醒我们那些难办的问题, 让我们按照出版业所要求的水平去做, 而至少我对于这种水平还不能自然适应.

到 2004 年初, 我们天真地以为已经到了编辑工作的后期, 而现在我才懂得, 其实还只是接近开始, 哪怕有 June 的帮助, 我们认识到需要我做的事情还多得很. 这

时, 我突然想起了一个人可以做理想的副主编, 他就是 Imre Leader, 我知道, 他懂得这本书想要达到什么, 以及怎样去达到. 他同意了, 很快就成了编辑团队不可少的一员, 他还委托别人并且自己也编写了好几个条目.

到了 2007 年下半年, 我们确实是到了后期. 这时可以看得很清楚, 如果再有外加的编辑方面的帮助, 就可以使得结束这项我们已经拖过了日期的细致的工作, 把书真正写完, 变得容易得多. Jordan Ellenberg 和陶哲轩 (Terence Tao) 同意来帮助, 他们的贡献是无价的. 他们编辑了一些条目, 自己写了另一些, 还帮助我写了几条在我专业领域之外的主题的短条目, 而且因为知道有他们在, 就不会发生大的错误, 所以我在知识上就放心了 (如果没有他们的帮助, 我可能要犯几个错误, 但是对于仍然漏网的错误, 我要负全责). 编者们写的条目都没有署名, 但是在撰稿人名录下方有一个注, 说明那些条目是哪位编者写的.

9. 编辑过程

要找到这样的数学家, 既有耐心又能理解对方, 能这样来向非专家和其他领域的同事来解释他们在做什么, 这并不是一件容易事. 数学家时常会假设对方知道什么事, 而其实他们并不知道, 要承认自己完全听糊涂了, 也使人难堪. 然而本书的编者曾经努力把这种听不懂的负担自己担起来. 本书的一个重要特点在于它的编辑过程是一个非常主动的过程: 我们没有简单地把条目委托出去, 然后收到什么就算什么. 有些稿子被完全抛开了, 而新条目按照编者的评论重新写过. 另一些需要做本质的改动, 有时是撰稿人来改, 有时则是编者来改. 少数条目只做了很无谓的改动就接受了, 但这只是极小的一部分.

撰稿人对于这样的处理表现出忍耐, 甚至谢意, 这对于编者一直是很受欢迎的惊喜, 而且帮助编者在编辑本书的好多年里, 能够坚持他们的原则. 我们想回过头来向撰稿人表达我们的谢意, 也希望他们同意认为这个过程还是值得的. 对于我们, 对于条目付出了这么大量的工作, 而没有实实在在的回报是不可想象的. 这里不是我自己来吹嘘, 在作者自认为结果是如何成功的地方, 但是在可接受性方面还需要做的改动之多, 这种干预性的编辑工作在数学上又是如此罕见, 我无法看出, 这本书怎么会不是在好的方向上非同寻常.

要想看一看每件事花了多么长时间, 看到撰稿人的水平, 一个标志就是有那么多撰稿人, 自从接受约稿以来, 得到了很大的奖赏和荣誉. 至少有三位撰稿人在写作时喜得贵子. 令人悲痛的是, 有两位撰稿人: Benjamin Yandel 和 Graham Allan, 未能在他们有生之年亲眼看见自己的文章成书, 但是我们希望这本书, 虽然微小, 却是对他们的纪念.

10. 致　谢

编辑过程的最初阶段当然是计划本书和找寻作者. 如果不是以下各位的帮助与建议, 这是不可能完成的. 他们是: Donald Albers, Michael Atiyah, Jordan Ellenberg, Tony Gardiner, Sergiu Klainerman, Barry Mazur, Curt McMullen, Robert O'Malley, 陶哲轩 (Terence Tao), 还有 Ave Wigderson , 他们都给出了建议, 这些建议对于本书的成形, 在某个方面有着良好的效果. June Barrow-Green 在她的工作中得到了 Jeremy Gray 和 Reinhard Siegmund-Schultze 的极大帮助. 在最后几个星期里, 承 Vicky Neale 善意担负了部分清样的校阅, 她在这方面的能力真令人吃惊, 找出了那么多万个我们自己绝看不出来的错误, 我们当然很愉快地改正了. 有许多数学家和数学史家耐心地回答了编者们的问题, 这个名单很长, 我们再次向他们深致谢意.

我要感谢许多人对我的鼓励, 包括本书所有的撰稿人和我身边的家人, 特别是我的父亲: Patrick Gowers, 这些鼓励使我能一往直前, 哪怕这个任务如同大山一样. 我还要感谢 Julie Barrau, 她的帮助虽不那么直接, 却也同样不可少. 在编书的最后几个月里, 她负担了远远超出她的份额的家务. 由于 2007 年 11 月儿子的出生, 这大大改变了我的生活, 正如她已经改变了我的生活一样.

撰 稿 人

谱 [Ⅲ.86]	**Graham Allan**, late Reader in Mathematics, University of Cambridge
极值与概率组合学 [Ⅳ.19]	**Noga Alon**, Baumritter Professor of Mathematics and Computer Science, Tel Aviv University
拉玛努金 [Ⅵ.82]	**George Andrews**, Evan Pugh Professor in the Department of Mathematics, The Pennsylvania State University
数学分析的严格性的发展 [Ⅱ.5] 厄尔米特 [Ⅵ.47]	**Tom Archibald**, Professor, Department of Mathematics, Simon Fraser University
霍奇 [Ⅵ.90] 对青年数学家的建议 [Ⅷ.6]	**Sir Michael Atiyah**, Honorary Professor, School of Mathematics, University of Edinburgh
布尔巴基 [Ⅵ.96]	**David Aubin**, Assistant Professor, institut de Mathématiques de Jussieu
集合理论 [Ⅳ.22]	**Joan Bagaria**, ICREA Research Professor, University of Barcelona
欧几里得算法和连分数 [Ⅲ.22] 优化与拉格朗日乘子 [Ⅲ.64] 高维几何学及其概率类比 [Ⅳ.26]	**Keith Ball**, Astor Professor of Mathematics, University College London
黎曼曲面 [Ⅲ.79]	**Alan F. Beardon**, Professor of Complex Analysis, University of Cambridge
模空间 [Ⅳ.8]	**David D. Ben-Zvl**, Associate Professor of Mathematics, University of Texas, Austin
遍历定理 [Ⅴ.9]	**Vitaly Bergelson**, Professor of Mathematics, The Ohio State University
科尔莫戈罗夫 [Ⅵ.88]	**Nicolas Bingham**, Professor, Mathematics Department, Imperial College London
哈代 [Ⅵ.73] 李特尔伍德 [Ⅵ.79] 对青年数学家的建议 [Ⅷ.6]	**Béla Bollobás**, Professor of Mathematics, University of Cambridge and University of Memphis
笛卡儿 [Ⅵ.11]	**Henk Bos**, Honorary Professor, Department of Science Studies, Aarhus University, Professor Emeritus, Department of Mathematics, Utrecht University
动力学 [Ⅳ.14]	**Bodil Branner**, Emeritus Professor, Department of Mathematics, Technical University of Denmark
几何和组合群论 [Ⅳ.10]	**Martin R. Bridson**, Whitehead Professor of Pure Mathematics, University of Oxford

数学的分析与哲学的分析 [Ⅶ.12]	**John P. Burgess**, Professor of Philosophy, Princeton University
L 函数 [Ⅲ.47], 模形式 [Ⅲ.59]	**Kevin Buzzard**, Professor of Pure Mathematics, Imperial College London
设计 [Ⅲ.14], 哥德尔定理 [Ⅴ.15]	**Peter J. Cameron**, Professor of Mathematics, Queen Mary, University of London
算法 [Ⅱ.4]	**Jean-Luc Chabert**, Professor, Laboratoire Amiénois de Mathématique Fondamentale et Appliquée, Universite de Picardie
范畴 [Ⅲ.8]	**Eugenia Cheng**, Lecturer, Department of Pure Mathematics, University of Sheffield
数学与密码 [Ⅶ.7]	**Clifford Cocks**, Chief Mathematician, Government Communications Headquarters, Cheltenham
对青年数学家的建议 [Ⅷ.6]	**Alain Connes**, Professor, Collège de France, IHES, and Vanderbilt University
证明的概念的发展 [Ⅱ.6]	**Leo Corry**, Director, The Cohn Institute for History and Philosophy of Science and Ideas, Tel Aviv University
冯 · 诺依曼 [Ⅵ.91]	**Wolfgang Coy**, Professor of Computer Science, Humboldt-Universitdt zu Berlin
凯莱 [Ⅵ.46]	**Tony Crilly**, Emeritus Reader in Mathematical Sciences, Department of Economics and Statistics, Middlesex University
毕达哥拉斯 [Ⅵ.1], 欧几里得[Ⅵ.2], 阿基米德 [Ⅵ.3], 阿波罗尼乌斯 [Ⅵ.4]	**Serafina Cuomo**, Lecturer in Roman History, School of History Classics and Archaeology, Birkbeck College
广义相对论和爱因斯坦 方程 [Ⅵ.13]	**Mihalis Dafermos**, Reader in Mathematical Physics, University of Cambridge
数学和经济的推理 [Ⅶ.8]	**Partha Dasgupta**, Frank Ramsey Professor of Economics, University of Cambridge
小波及其应用 [Ⅶ.3]	**Ingrid Daubechies**, Professor of Mathematics, Princeton University
康托 [Ⅵ.54], 鲁宾逊 [Ⅵ.95]	**Joseph W. Dauben**, Distinguished Professor, Herbert H. Lehman College and City University of New York
哥德尔 [Ⅵ.92]	**John W. Dawson Jr.**, Professor of Mathematics, Emeritus, The Pennsylvania State University
达朗贝尔 [Ⅵ.20]	**Francois de Gandt**, Professeur d'Histoire des Sciences et de Philosophie, University Charles de Gaulle, Lille
数理统计学 [Ⅶ.10]	**Persi Diaconis**, Mary V. Sunseri Professor of Statistics and Mathematics, Stanford University
椭圆曲线 [Ⅲ.21], 概型 [Ⅲ.82], 算术几何 [Ⅳ.5]	**Jordan S. Ellenberg**, Associate Professor of Mathematics, University of Wisconsin

变分法 [Ⅲ.94]	**Lawrence C. Evans**, Professor of Mathematics, University of California, Berkeley
数学与艺术 [Ⅶ.14]	**Florence Fasanelli**, Program Director, American Association for the Advancement of Science
塔尔斯基 [Ⅵ.87]	**Anita Burdman Feferman**, Independent Scholar and Writer, Solomon Feferman, Patrick Suppes Family Professor of Humanities and Sciences and Emeritus Professor of Mathematics and Philosophy, Department of Mathematics, Stanford University
欧拉方程和纳维-斯托克斯方程[Ⅲ.23], 卡尔松定理 [Ⅴ.5]	**Charles Fefferman**, Professor of Mathematics, Princeton University
阿廷 [Ⅵ.86]	**Della Fenster**, Professor, Della Fenster, Professor, Department of Mathematics and Computer Science, University of Richmond, Virginia
数学基础中的危机 [Ⅱ.7], 戴德金 [Ⅵ.50], 佩亚诺 [Ⅵ.62]	**José Ferreirós**, Professor of Logic and Philosophy of Science, University of Seville
Mostow 强刚性定理 [Ⅴ.23]	**David Fisher**, Associate Professor of Mathematics, Indiana University, Bloomington
顶点算子代数 [Ⅳ.17]	**Terry Gannon**, Professor, Department of Mathematical Sciences, University of Alberta
解题的艺术 [Ⅷ.1]	**A. Gardiner**, Reader in Mathematics and Mathematics Education, University of Birmingham
拉普拉斯 [Ⅵ.23]	**Charles C. Gillispie**, Dayton-Stockton Professor of History of Science, Emeritus, Princeton University
计算复杂性 [Ⅳ.20]	**Oded Goldreich**, Professor of Computer Science, Weizmann Institute of Science, Israel
费马 [Ⅵ.12]	**Catherine Goldstein**, Directeur de Recherche, Institut de Mathématiques de Jussieu, CNRS, Paris
从数到数系 [Ⅱ.1], 数论中的局部与整体 [Ⅲ.51]	**Fernando Q. Gouvêa**, Carter Professor of Mathematics, Colby College, Waterville, Maine
解析数论 [Ⅳ.2]	**Andrew Granville**, Professor, Department of Mathematics and Statistics, Université de Montreal
勒让德 [Ⅵ.24], 傅里叶 [Ⅵ.25], 泊松 [Ⅵ.27], 柯西 [Ⅵ.29], 罗素 [Ⅵ.71], 里斯 [Ⅵ.74]	**Ivor Grattan-Guinness**, Emeritus Professor of the History of Mathematics and Logic, Middlesex University
几何学 [Ⅱ.2], 富克斯群 [Ⅲ.28], 高斯 [Ⅵ.26], 莫比乌斯 [Ⅵ.30], 罗巴切夫斯基 [Ⅵ.31], 波尔约[Ⅵ.34], 黎曼 [Ⅵ.49], 克利福德 [Ⅵ.55], 嘉当 [Ⅵ.69], 斯科伦 [Ⅵ.81]	**Jeremy Gray**, Professor of History of Mathematics, The Open University

Gamma 函数 [Ⅲ.31], 无理数和超越数 [Ⅲ.41], 模算术 [Ⅲ.58], 数域 [Ⅲ.63], 二次型 [Ⅲ.73], 拓扑空间 [Ⅲ.90], 三角函数 [Ⅲ.92]	**Ben Green**, Herchel Smith Professor of Pure Mathematics, University of Cambridge
表示理论 [Ⅳ.9]	**Ian Grojnowski**, Professor of Pure Mathematics, University of Cambridge
牛顿 [Ⅵ.14]	**Niccolò Guicciardini**, Associate Professor of History of Science, University of Bergamo
您会问"数学是为了什么"[Ⅷ.2]	**Michael Harris**, Professor of Mathematics, Université Paris 7-Denis Diderot
狄利克雷 [Ⅵ.36]	**Ulf Hashagen**, Doctor, Munich Center for the History of Science and Technology, Deutsches Museum, Munich
算子代数 [Ⅳ.15], 阿蒂亚–辛格指标定理 [Ⅴ.2]	**Nigel Higson**, Professor of Mathematics, The Pennsylvania State University
图灵 [Ⅵ.94]	**Andrew Hodges**, Tutorial Fellow in Mathematics, Wadham College, University of Oxford
辫群 [Ⅲ.4]	**F. E. A. Johnson**, Professor of Mathematics, University College London
货币的数学 [Ⅶ.9]	**Mark Joshi**, Associate Professor, Centre for Actuarial Studies, University of Melbourne
从二次互反性到类域理论 [Ⅴ.28]	**Kiran S. Kedlaya**, Associate Professor of Mathematics, Massachusetts Institute of Technology
网络中的流通的数学 [Ⅶ.4]	**Frank Kelly**, Professor of the Mathematics of Systems and Master of Christ's College, University of Cambridge
偏微分方程 [Ⅳ.12]	**Sergiu Klainerman**, Professor of Mathematics, Princeton University
算法设计的数学 [Ⅶ.5]	**Jon Kleinberg**, Professor of Computer Science, Cornell University
魏尔斯特拉斯 [Ⅵ.44]	**Israel Kleiner**, Professor Emeritus, Department of Mathematics and Statistics, York University
数学与化学 [Ⅶ.1]	**Jacek Klinowski**, Professor of Chemical Physics, University of Cambridge
莱布尼兹 [Ⅵ.15]	**Eberhard Knobloch**, Professor, Institute for Philosophy, History of Science and Technology, Technical University of Berlin
代数几何 [Ⅳ.4]	**János Kollar**, Professor of Mathematics, Princeton University
特殊函数 [Ⅲ.85], 变换 [Ⅲ.91], 巴拿赫–塔尔斯基悖论 [Ⅴ.3], 数学的无处不在 [Ⅷ.3]	**T. W. Körner**, Professor of Fourier Analysis, University of Cambridge

极值与概率组合学 [Ⅳ.19]	**Michael Krivelevich**, Professor of Mathematics, Tel Aviv University
柯朗 [Ⅵ.83]	**Peter D. Lax**, Professor, Courant Institute of Mathematical Sciences, New York University
随机过程 [Ⅳ.24]	**Jean-François Le Gall**, Professor of Mathematics, University Paris-Sud, Orsay
纽结多项式 [Ⅲ.44]	**W. B. R. Lickorish**, Emeritus Professor of Geometric Topology, University of Cambridge
置换群 [Ⅲ.68], 有限单群的分类[Ⅴ.7], 五次方程的不可解性 [Ⅴ.21]	**Martin W. Liebeck**, Professor of Pure Mathematics, Imperial College London
刘维尔 [Ⅵ.39]	**Jesper Lutzen**, Professor, Department of Mathematical Sciences, University of Copenhagen
布尔 [Ⅵ.43]	**Des MacHale**, Associate Professor of Mathematics, University College Cork
数学与化学 [Ⅶ.1]	**Alan L. Mackay**, Professor Emeritus, School of Crystallography, Birkbeck College
量子群 [Ⅲ.75]	**Shahn Majid**, Professor of Mathematics, Queen Mary, University of London
巴拿赫 [Ⅵ.84]	**Lech Maligranda**, Professor of Mathematics, Luleà University of Technology, Sweden
逻辑和模型理论 [Ⅵ.23]	**David Marker**, Head of the Department of Mathematics, Statistics, and Computer Science, University of Illinois at Chicago
瓦莱·布散 [Ⅵ.67]	**Jean Mawhin**, Professor of Mathematics, University Catholique de Louvain
代数数 [Ⅵ.1]	**Barry Mazur**, Gerhard Gade University Professor, Mathematics Department, Harvard University
对青年数学家的建议 [Ⅷ.6]	**Dusa McDuff**, Professor of Mathematics, Stony Brook University and Barnard College
艾米·诺特 [Ⅵ.76]	**Colin McLarty**, Truman P. Handy Associate Professor of Philosophy and of Mathematics, Case Western Reserve University
四色定理 [Ⅴ.12]	**Bojan Mohar**, Canada Research Chair in Graph Theory, Simon Fraser University, Professor of Mathematics, University of Ljubljana
阿贝尔 [Ⅵ.33], 伽罗瓦 [Ⅵ.41], 弗罗贝尼乌斯 [Ⅵ.58], 伯恩塞德 [Ⅵ.60]	**Peter M. Neumann**, Fellow and Tutor in Mathematics, The Queen's College, Oxford, University Lecturer in Mathematics, University of Oxford
数学与音乐 [Ⅶ.13]	**Catherine Nolan**, Associate Professor of Music, The University of Western Ontario

概率分布 [Ⅲ.71]	**James Norris**, Professor of Stochastic Analysis, Statistical Laboratory, University of Cambridge
韦伊猜想 [Ⅴ.35]	**Brian Osserman**, Assistant Professor, Department of Mathematics, University of California, Davis
线性与非线性波以及孤子 [Ⅲ.49]	**Richard S. Palais**, Professor of Mathematics, University of California, Irvine
拉格朗日 [Ⅵ.22]	**Marco Panza**, Directeur de Recherche, CNRS, Paris
抽象代数的发展 [Ⅱ.3], 西尔维斯特 [Ⅵ.42]	**Karen Hunger Parshall**, Professor of History and Mathematics, University of Virginia
辛流形 [Ⅲ.88]S	**Gabriel P. Paternain**, Reader in Geometry and Dynamics, University of Cambridge
伯努利家族 [Ⅵ.18]	**Jeanne Peiffer**, Directeur de Recherche, CNRS, Centre Alexandre Koyri, Paris
克罗内克 [Ⅵ.48], 韦伊 [Ⅵ.93]	**Birgit Petri**, Ph.D. Candidate, Fachbereich Mathematik, Technische Universitdt Darmstadt
计算数论 [Ⅵ.3]	**Carl Pomerance**, Professor of Mathematics, Dartmouth College
雅可比 [Ⅵ.35]	**Helmut Pulte**, Professor, Ruhr-Universitdt Bochum
Robertson-Seymour 定理[Ⅴ.32]	**Bruce Reed**, Canada Research Chair in Graph Theory, McGill University
数理生物学 [Ⅶ.2]	**Michael C. Reed**, Bishop-MacDermott Family Professor of Mathematics, Duke University
数学大事年表 [Ⅷ.7]	**Adrian Rice**, Associate Professor of Mathematics, Randolph-Macon College, Virginia
数学意识 [Ⅷ.4]	**Eleanor Robson**, Senior Lecturer, Department of History and Philosophy of Science, University of Cambridge
热方程 [Ⅲ.36]	**Igor Rodnianski**, Professor of Mathematics, Princeton University
算子代数 [Ⅵ.15], 阿蒂亚-辛格指标定理 [Ⅴ.2]	**John Roe**, Professor of Mathematics, The Pennsylvania State University
建筑 [Ⅲ.5], 李的理论 [Ⅲ.48]	**Mark Ronan**, Professor of Mathematics, University of Illinois at Chicago; Honorary Professor of Mathematics, University College London
欧拉 [Ⅵ.19]	**Edward Sandifer**, Professor of Mathematics, Western Connecticut State University
对青年数学家的建议 [Ⅷ.6]	**Peter Sarnak**, Professor, Princeton University and Institute for Advanced Study, Princeton
闵可夫斯基 [Ⅵ.64]	**Tilman Sauer**, Doctor, Einstein Papers Project, California Institute of Technology
克罗内克 [Ⅵ.48], 韦伊 [Ⅵ.93]	**Norbert Schappacher**, Professor, Institut de Recherche Mathematique Avancee, Strasbourg

谢尔品斯基 [Ⅵ.77]	**Andrzej Schinzel**, Professor of Mathematics, Polish Academy of Sciences
豪斯道夫 [Ⅵ.68], 外尔 [Ⅵ.80]	**Erhard Scholz**, Professor of History of Mathematics, Department of Mathematics and Natural Sciences, Universität Wuppertal
勒贝格 [Ⅵ.72], 维纳 [Ⅵ.85]	**Reinhard Siegmund-Schultze**, Professor, Faculty of Engineering and Science, University of Agder, Norway
临界现象的概率模型 [Ⅵ.25]	**Gordon Slade**, Professor of Mathematics, University of British Columbia
数学与医学统计 [Ⅶ.11]	**David J. Spiegelhalter**, Winton Professor of the Public Understanding of Risk, University of Cambridge
维特 [Ⅵ.9]	**Jacqueline Stedall**, Junior Research Fellow in Mathematics, The Queen's College, Oxford
李 [Ⅵ.53]	**Arild Stubhaug**, Freelance Writer, Oslo
信息的可靠传输 [Ⅶ.6]	**Madhu Sudan**, Professor of Computer Science and Engineering, Massachusetts Institute of Technology
紧性与紧化 [Ⅲ.9], 微分形式和积分 [Ⅲ.16], 广义函数 [Ⅲ.18], 傅里叶变换 [Ⅲ.27], 函数空间 [Ⅲ.29], 哈密顿函数 [Ⅲ.35], 里奇流 [Ⅲ.78], 薛定谔方程 [Ⅲ.83], 调和分析 [Ⅳ.11]	**陶哲轩 (Terence Tao)**, Professor of Mathematics, University of California, Los Angeles
弗雷格 [Ⅵ.56]	**Jamie Tappenden**, Associate Professor of Philosophy, University of Michigan
微分拓扑 [Ⅳ.7]	**C. H. Taubes**, William Petschek Professor of Mathematics, Harvard University
克莱因 [Ⅵ.57]	**Rüdiger Thiele**, Privatdozent, Universitat Leipzig
代数拓扑 [Ⅳ.6]	**Burt Totaro**, Lowndean Professor of Astronomy and Geometry, University of Cambridge
数值分析 [Ⅳ.21]	**Lloyd N. Trefethen**, Professor of Numerical Analysis, University of Oxford
布劳威尔 [Ⅵ.75]	**Dirk van Dalen**, Professor, Department of Philosophy, Utrecht University
单形算法 [Ⅲ.84]	**Richard Weber**, Churchill Professor of Mathematics for Operational Research, University of Cambridge
拟阵 [Ⅲ.54]	**Domimc Welsh**, Professor of Mathematics, Mathematical Institute, University of Oxford
伸展图 [Ⅲ.24], 计算复杂性 [Ⅳ.20]	**Avi Wigderson**, Professor in the School of Mathematics, Institute for Advanced Study, Princeton
数学: 一门实验科学 [Ⅷ.5]	**Herbert S. Wilf**, Thomas A. Scott Professor of Mathematics, University of Pennsylvania

哈密顿 [VI.37]	**David Wilkins**, Lecturer in Mathematics, Trinity College, Dublin
希尔伯特 [VI.63]	**Benjamin H. Yandell**, Pasadena, California (已去世)
Calabi-Yau 流形 [III.6], 镜面对称 [IV.16]	**Eric Zaslow**, Professor of Mathematics, Northwestern University
列举组合学与代数组合学 [IV.18]	**Doron Zeilberger**, Board of Governors Professor of Mathematics, Rutgers University

未署名的条目是编者们写的. 在第III部分里, 以下各条是 Imre Leader 撰写的: 选择公理[III.1], 决定性公理[III.2], 基数[III.7], 可数与不可数集合[III.11], 图[III.34], 约当法式[III.43], 测度[III.55], 集合理论的模型[III.57], 序数[III.66], 佩亚诺公理[III.67], 环, 理想与模[III.81], 策墨罗–费朗克尔公理[III.99]. 在第V部分里, 连续统假设的独立性[V.18] 是 Imre Leader 撰写的; 三体问题[V.33] 则是 June Barrow-Green 撰写的. 在第VI部分里, June Barrow-Green 撰写了所有未署名的条目; 全书其他所有未署名的条目都是 Timothy Gowers 撰写的.

目　录

第 I 部分　引　论

I.1　数学是做什么的

要对“什么是数学”这样一个问题给出一个令人满意的回答, 其困难是众所周知的. 本书的处理途径是：不试图去回答它. 我们不打算给出数学的定义, 而是通过描述它的许多最重要的概念、定理和应用, 使得对于什么是数学有一个好的看法. 然而, 想使这些材料的信息有意义, 对于数学的内容作某种分类还是有必要的.

对数学进行分类最明显的方法是按照其内容来进行. 这篇简短的引论以及下面比较长的条目如一些基本的数学定义 [I.3]就是采取的这个方法. 但是, 这并不是唯一的方法, 甚至显然也不是最好的方法. 另一种途径是按照数学家们喜欢思考的问题的类型来分类, 这会给这门学科以一种不同的视角, 而这是很有用的, 时常有这样的情况, 两个数学领域, 如果您只注意它们的主题材料, 可能看起来很不相同, 但是如果您看一看它们考察的问题, 则又十分相似. 第 I 部分的最后一个条目数学研究的一般目的 [I.4]就是从这个观点来观察数学的. 在那篇文章末尾有一个简短的讨论, 您可以把它看成是第三种分类, 就是并不对数学本身来分类, 而是对数学期刊的一篇典型论文内容的各个部分来分类. 这篇论文里既有定理和证明, 也有定义、例子、引理、公式、猜想等等. 那里讨论的要点就是想说明这些词是什么意思, 以及为什么数学的产出物里面的这些东西也是很重要的.

1. 代数、几何和分析

虽然一旦想把数学主题分类, 就必定立即需要加上种种限制. 然而有一个粗略的分类无疑可以作为最初的近似, 这就是把数学分成代数、几何和分析. 所以我们就以此开始, 以后再作各种修饰.

1.1　代数与几何的对比

绝大多数读过中学的人都会把代数看成用字母代表数所得到的数学. 时常会把代数与算术作一个对照：算术就是对数作更直接的研究. 所以“$3\times 7=?$”这样的问题就被认为是属于算术的, 而“若 $x+y=10$, 而 $xy=21$, 则 x 与 y 中较大的一个取何值”就被看作是代数. 在比较高水平的数学里面, 这个对比就不那么显眼, 原因也很简单, 因为数字单独出现而不与字母相伴是极为罕见的.

然而, 代数与几何之间就有着不同的对比, 而且它在比较高深的水平上要重要

得多. 中学里关于几何的概念是: 它是研究图形的, 例如圆、三角形、立方体和球面, 还有诸如旋转、反射、对称等等概念. 这样, 几何的对象以及这些对象所经历的过程, 比之代数的方程, 有着多得多的可视的特性.

这种对比一直持续到现代数学研究的前沿. 数学有些部分涉及按照某种规则对符号进行操作, 例如对于一个为真的等式, "如果对其双方作同样的操作", 则它仍然为真. 数学的这些部分, 典型地被认为是代数的一部分, 而另外一些牵涉到可视的概念的部分, 则典型地被认为是几何的一部分.

然而, 这样的区别绝不是简单的. 如果您看到一篇典型的几何研究的论文, 它会充满图形吗? 几乎绝对不会. 事实上, 用以解决几何问题的方法, 极为常见地涉及极为大量的符号操作, 但是, 找出与应用这些方法需要很好的可视化的能力, 在它的下面, 典型地有图形在. 至于代数, 它 "仅仅是" 符号演算吗? 完全不是这样. 非常常见的是, 人们解决代数问题是通过寻找一个办法把它可视化.

作为把代数问题可视化的例子, 想一下, 人们是怎样来验证 "当 a 和 b 都是正整数时, $ab = ba$". 可以把它作为一个纯粹的代数问题来处理 (例如用归纳法来证明它), 但是想要说服自己, 最容易的方法是想象一个矩形的阵, 阵中一共有 a 行, 而每一行有 b 个物件. 物件总数, 如果是逐行来数, 就可以认为是 a 批物件, 而每批 b 个; 如果是逐列来数, 就是有 b 批, 每批 a 个. 所以 $ab = ba$. 用类似的方法还可以验证其他的基本规则, 例如 $a(b + c) = ab + ac$, 以及 $a(bc) = (ab)c$.

转过头来, 事实上, 解决许多几何问题的好方法是 "把它转换成代数". 这种做法最著名的例子是使用笛卡儿坐标. 例如, 如果想把一个圆对经过圆心的直线 L 作反射, 再逆时针旋转 $40°$, 然后再对同一直线 L 反射一次. 这个问题的一种做法是把它可视化如下:

想象这个圆是用薄的木片做的. 不必对此直线反射, 而可以 (通过木片外的第 3 维) 绕 L 旋转 $180°$. 再把所得的结果翻一个面, 其实, 如果对木片的厚度忽略不计, 翻面并不起作用. 现在如果从木片下方往上看, 并且让它逆时针旋转 $40°$, 则从原来的位置看, 木片是顺时针旋转了 $40°$. 现在再把木片翻回来, 即绕 L 在第 3 维里再旋转 $180°$, 总的效果就是顺时针方向旋转 $40°$.

不同的数学家利用上面这种论证方法的意愿与能力是大不相同的. 如果您还不能充分可视地看出上面这种论证肯定是对的, 就会喜欢按照代数途径, 即利用线性代数和矩阵理论的方法 (详见 (I.3 §3.2)). 开始是把圆看成适合 $x^2 + y^2 \leqslant 1$ 的数对 (x, y) 的集合. 那两个变换, 即对通过圆心的直线 L 的反射, 以及旋转 $40°$ 都可以用 2×2 的矩阵 $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ 来表示. 有一个稍微复杂一点的纯粹代数的法则把矩阵乘起来, 而且这个法则就是这样来设计的, 使之有这样的性质: 如果矩阵 A 代表一个变换 R(比如说是反射), 而矩阵 B 表示另一个变换 T, 则乘积 AB 就表示先

作 T 再作 R 所得的变换. 因此我们可以这样来解决上面的问题: 写出相应于这些变换的矩阵, 把它们乘起来, 再看是什么变换相应于这个乘积. 几何问题就这样转换成了一个代数问题, 并且代数地解决.

这样, 尽管我们可以在几何与代数之间找出有用的区别, 可是不要以为二者的界限是非常清晰的. 事实上, 数学的一个主要的分支就叫做代数几何[IV.4]. 而上面的例子说明, 时常可以把一点数学从代数变成几何, 反过来也一样. 不论如何, 在代数和几何的思维方式之间有确定的区别 —— 一个比较注意符号, 一个比较注意图像 —— 这一点对于决定数学家追随哪个研究方向, 有深刻的影响.

1.2 代数与分析的对比

"分析" 一词, 若代表数学的一个分支, 则在中学水平上并不起大作用. 然而, "微积分" 这个词大家就熟悉得多, 而微分和积分是数学中划分为分析而非代数与几何的好例子. 理由在于它们都牵涉到极限过程. 例如函数 f 在 x 点的导数就是 f 的图像的弦的梯度①, 它是一个序列的极限. 而具有弯曲边界的形状的面积则定义为越来越充满这个形状的直边区域面积的极限 (这些概念将在 [I.3 §3.2] 里作详细得多的讨论).

这样, 作为最初步的近似, 可以说, 凡是一个数学分支涉及极限过程, 它就属于分析, 而如果只需通过有限多个步骤就能得到答案, 它就属于代数. 然而, 这个最初的近似, 又一次不仅是粗略的, 而且会产生误导, 理由也是类似的: 不是哪些数学分支应该分类为分析或代数, 应该分类的是数学技巧.

既然我们不可能写出无限长的证明, 又怎么能够证明任何一件关于极限过程的事呢? 为了回答这个问题, 让我们来看一看是怎样来论证一个简单的命题, 即 x^3 的导数是 $3x^2$ 的. 通常的论证是, 连接两点 (x, x^3) 和 $((x+h), (x+h)^3)$ 的弦的梯度是

$$\frac{(x+h)^3 - x^3}{x+h-x},$$

计算以后得到 $3x^2+3xh+h^2$. 当 h"趋于零时", 这个梯度 "趋于 $3x^2$", 所以我们说在 x 点, 梯度就是 $3x^2$. 但是如果我们还想仔细一点又将如何? 比方说, 当 x 为很大时, 略去 $3xh$ 这一项还有根据吗?

为了打消疑虑, 我们再稍作一点运算来证明不论 x 取何值, $3xh+h^2$ 这一项总能够变得任意小, 只要 h 充分小就行了. 下面是做这件事的方法之一. 设固定一个小的正数 ε, 这里的 ε 表示我们能够容忍的误差的限度, 则若 $|h| \leqslant \varepsilon/6|x|$, 就有 $|3xh| \leqslant \varepsilon/2$. 如果我们再有 $|h| \leqslant \sqrt{\varepsilon/2}$, 则又有 $h^2 \leqslant \varepsilon/2$. 所以只要 h 小于 $\varepsilon/6|x|$ 和 $\sqrt{\varepsilon/2}$ 中的较小者, $3x^2+3xh+h^2$ 和 $3x^2$ 之差就至多是 ε.

① 即斜率. —— 中译本注

上面的论证有两个特点在分析中是典型的. 第一, 虽然我们想要证明的命题是关于极限过程的, 所以是 "无穷性"(infinitary) 的, 我们为证明它所必须做的工作则完全是有限的. 第二, 这个工作的本质是寻求某个相当简单的不等式 (现在是 $|3xh+h^2|\leqslant\varepsilon$) 成立的充分条件.

让我们再举一个例子来说明第二个特点: 证明对于每一个实数 x, $x^4-x^2-6x+10$ 均为正数. 下面是一个 "分析学论证". 首先注意到, 若 $x\leqslant -1$, 则 $x^4\geqslant x^2$, 同时 $10-6x\geqslant 0$, 所以这时结果一定为真. 若 $-1\leqslant x\leqslant 1$, 则 $|x^4-x^2-6x|$ 不能大于 $x^4+x^2+6|x|$, 而后者最多为 8, 所以 $x^4-x^2-6x\geqslant -8$, 由此可得 $x^4-x^2-6x+10\geqslant 2$. 若 $1\leqslant x\leqslant 3/2$, 则 $x^4\geqslant x^2$ 且 $6x\leqslant 9$, 从而 $x^4-x^2-6x+10\geqslant 1$. 若 $3/2\leqslant x\leqslant 2$, 则 $x^2\geqslant 9/4$, 所以 $x^4-x^2=x^2(x^2-1)\geqslant \dfrac{9}{4}\cdot\dfrac{5}{4}>2$. 还有 $6x\leqslant 12$, 故 $10-6x\geqslant -2$, 所以 $x^4-x^2-6x+10>0$. 最后, 若 $x\geqslant 2$, 则 $x^4-x^2=x^2(x^2-1)\geqslant 3x^2\geqslant 6x$, 由此可得 $x^4-x^2-6x+10\geqslant 10$.

上面的证明有点长, 但是每一步都是证明一个相当简单的不等式, 这就是说上述证明是一个典型的分析证明的意义. 作为对照, 这里再给出一个 "代数学家" 的证明. 只要注意到 $x^4-x^2-6x+10$ 其实等于 $(x^2-1)^2+(x-3)^3$, 所以它总是正的.

如果可以在代数和分析中作一个选择, 似乎人们总会赞成代数. 不论如何, 代数证明要短多了, 而使得这个函数很明显地为正. 然而, 分析学家的证明虽然有好几步, 但每一步都很简单, 代数证明的简短反而会产生误导, 因为它对于怎样找到等价的式子 $(x^2-1)^2+(x-3)^3$ 没有给出任何线索. 而且, 事实上, 一个多项式写为其他多项式平方之和这个一般问题却是既有趣又困难的问题 (特别是在多项式的变元多于一个的情况).

处理这个问题还有第三种混合的途径, 这就是用微积分找到使 $x^4-x^2-6x+10$ 达到最小值的点. 这里的想法就是: 先求出导数 $4x^3-2x+6$(这是一个经过了分析论证的代数过程), 求出它的根 (这是代数), 再验证 $x^4-x^2-6x+10$ 在此点的值为正. 然而, 虽然这个方法对于许多问题是好方法, 现在却需要一点技巧, 因为三次多项式 $4x^3-2x+6$ 没有整数根. 但是我们可以用分析的论证, 找到最小值一定出现在其中的小区间, 这就会减少用第一种纯分析论证时, 需要分别考虑的情况的个数.

正如这个例子所示, 虽然分析时常涉及极限过程, 而代数则不, 二者之间的一个更加显著的区别在于: 代数学家喜欢与准确的公式打交道, 分析学家则喜欢作估计. 或者说得更加简洁一点: 代数学家喜欢等式, 分析学家喜欢不等式.

2. 数学的主要分支

既已讨论了代数、几何和分析的思维方式的区别, 我们就已准备好对数学的主题作一个粗略的分类. 我们面临着一个可能的混乱, 因为 "代数"“几何” 和 "分析" 这些词既表示特定的数学分支, 又表示一种贯穿于许多不同分支的思维方式. 所以,

说分析的某些分支比其他分支更加代数化 (或者更加几何化) 还是有意义的 (而且是真的). 类似于此, 代数拓扑学几乎完全是代数的, 但是性质却是几何的, 而其研究的对象 —— 拓扑空间, 又是分析的一部分, 这样说也不是悖论. 在本节中, 我们主要是按照主题来思考, 但是重要的是要记住前一节里讲的特点, 记得这些主题在某种意义下更加基本. 我们的描述是非常简要的, 关于数学的主要分支, 进一步阅读的材料, 可以在第Ⅱ和第Ⅳ部分里找到, 一些更加精确之处, 可以见于第 III 和第 V 部分的讨论.

2.1 代数

用 “代数” 一词来表示一个数学分支, 其含义比用这个词来表示对于符号运算和等式的偏好还要更确切一些. 代数学家关心的是数系、多项式, 以及更抽象的结构, 如群、域、向量空间和环 (在条目*一些基本的数学定义* [I.3]里有较详细的讨论). 从历史上看, 这些抽象的结构是从具体的例子中推广而得的. 例如, 在所有整数的集合与具有 (例如有理系数) 的多项式集合之间有着重要的类同, 这两个集合都是一种所谓欧几里得域的代数结构之例. 这个事实就把这个类同展现出来了. 如果对于欧几里得域有了较好的理解, 就可以把这个理解同时应用于整数和多项式.

这就突出了出现于许多数学分支的一种对立, 即一般的、抽象的命题与特殊的、具体的命题的对立. 一位代数学家考虑群, 可以是为了理解一个特定的复杂的对称群, 而另一位则可能是因为群是数学对象的一个基本类别而对其一般理论感兴趣. 抽象代数是从具体问题发展起来的, 关于这个发展, 可见*现代代数的来源* [Ⅱ.3].

关于第一种情况, 即研究群是为了理解一个特定的复杂的对称群, 一个绝佳的例子是*五次方程的不可解性* [V.21]—— 结果是证明了不存在一个把五次多项式的根用它的系数表示出来的公式. 我们是通过分析与多项式的根相关的对称性, 并理解这个对称性所成的群, 来证明这个定理的. 这个具体的群 (说一类群更好, 因为对于每个多项式各有一个群) 的例子在群的抽象理论的发展中起了重要的作用.

至于第二类定理, 即把群作为数学对象的一个基本类别来研究, 则*有限单群的分类* [V.7]是一个好例子, 它描述了基本的构造单元, 而每一个有限群都是由这些单元构建起来的.

代数结构在整个数学中都会出现, 代数对于其他领域如数论、几何, 甚至数学物理, 有许多应用.

2.2 数论

数论大量考虑的是正整数的集合, 这样, 就和代数有很大的重叠. 但是方程 $13x-7y=1$ 这个简单的例子可以说明一个典型的代数问题和一个典型的数论问题的区别. 一个代数学家会简单地只是注意到, 它的解是一个单参数族: 若 $y=\lambda$,

则 $x=(1+7\lambda)/13$, 所以通解是 $(x,y)=((1+7\lambda)/13,\lambda)$. 一个数论学家感兴趣的可能只是它的整数解, 所以就要搞清楚, 对于哪些整数 λ, $1+7\lambda$ 是 13 的倍数 (答案是, $1+7\lambda$ 是 13 的倍数, 当且仅当 λ 可以写为 $13m+11$ 的形式, 这里 m 是一个整数).

然而, 这样的描述对于现代数论不太公正, 因为数论已经成了一个高度精巧的学科. 绝大多数数论学家并不直接试图用整数去解方程, 而是努力去理解种种结构, 这些结构原来是为了研究这种方程而发展起来的, 现在自己有了生命, 成了有其自身价值的研究对象. 这个过程有时会重复若干次, 所以 "数论" 这个词, 对于数论学家之所作所为, 给出了一个容易产生误导的图景. 尽管如此, 这个学科的最抽象的部分也常有最实实在在的应用. 怀尔斯 (Andrew Wiles) 关于费马大定理 [V.10]的著名的证明就是一个显著的例子.

有趣的是, 按照这里的讨论的观点, 数论有两个颇不相同的子分支: 代数数论[IV.1]和解析数论 [IV.2]. 有一个粗略的经验规则: 研究方程的整数解引导到代数数论, 而解析数论的根源是素数的研究, 当然, 真实的图景要复杂得多.

2.3　几何

几何学研究的中心对象是流形, 关于它的讨论见 [I.3 §6.9]. 流形是例如球面这样的几何形体在高维的推广, 流形的每一个小部分看起来都是平坦的, 但是整体上看起来可以弯曲得非常复杂. 绝大多数自称为几何学家的人都在以这种或那种方式研究流形. 和代数的情况一样, 有些人对特殊的流形有兴趣, 有些人则对比较一般的理论有兴趣.

在研究流形时, 可以依据何时可以把两个流形看成是 "真正不同" 而作进一步的分类, 依据的是何时可以把两个流形看成是 "真正不同的" 流形. 如果两个对象可以连续地互相变形, 或者说, 可以用某种 "态映射"(morphism) 把一个变为另一个, 拓扑学家就认为它们是同样的, 例如苹果和梨对于拓扑学家就是同样的. 这意味着, 对于拓扑学家, 相对距离是不重要的, 因为可以用连续的拉伸来改变它. 一个微分拓扑学家还要求变形是 "光滑的"(这意味着它是 "充分可微的"). 这就造成了流形的更精细的分类, 产生出另一套问题. 在研究范围的另一个极端, 即 "更加几何" 的一端, 则有这样的数学家, 他们对流形上的点之间的距离 (这个概念对于拓扑学家没有意义) 的精确的本性兴趣大得多, 他们更加关心可以附加于流形上的辅助的构造. 在黎曼度量 [I.3 §6.10]和里奇流[III.78] 里, 可以找到对于几何学的更加几何化的东西的一点痕迹.

2.4　代数几何

从标题顾名思义就可以看出, 代数几何在上述分类里面没有显然的位置, 所以对它单独讨论比较容易一些. 代数几何学家也研究流形, 但与上面所说有重要的区

别, 就是他们的流形是由多项式来定义的 (这方面一个简单的例子是球面, 它可以定义为适合 $x^2 + y^2 + z^2 = 1$ 的 (x, y, z) 的集合). 这意味着, 代数几何从 “完全是关于多项式的” 这一点而言, 它是代数的, 但是从多变量多项式的解的集合是一个几何对象这一点而言, 它又是几何的.

代数几何的一个重要部分是对于奇异性的研究. 一个多项式方程组的解的集合时常相似于一个流形, 但有一些例外的奇点. 例如方程 $x^2 = y^2 + z^2$ 定义一个 (双叶) 锥面, 而在原点 $(0,0,0)$ 处有一个奇点. 如果观察锥面上一点 x 的邻域, 则只要 x 不是 $(0,0,0)$, 这个邻域就很像是平坦的平面. 然而, 若 x 是 $(0,0,0)$, 则不论这个邻域多么小, 仍然会看见锥的顶点在那儿. 这样, $(0,0,0)$ 是一个奇点 (这意味着锥面并不是一个真正的流形, 而是一个 “带有奇点的流形”).

正是代数和几何的交织构成代数几何的魅力的部分来源, 对这个学科的进一步的推动则来自它与其他数学分支的联系. 它与数论有特殊的联系, 这一点将在条目算术几何[IV.5] 中解释. 更加惊人的是它与数学物理有重要的联系, 条目镜面对称[IV.16]将讨论二者的某些联系.

2.5 分析

分析从一出现就带着多种不同的格调. 研究偏微分方程 [IV.12]是它的一个重大的主题. 这是因为发现了偏微分方程控制着许多物理过程, 例如引力场中的运动. 但是偏微分方程也在纯粹数学里出现 —— 特别是在几何学里面, 所以它催生了一个很大的数学分支, 而有许多子分支与许多其他领域相联系.

和代数一样, 分析也有其抽象的一面, 例如巴拿赫空间 [III.62]和希尔伯特空间 [III.37]、C^*-代数 [IV.15 §3]和冯 · 诺依曼代数 [IV.15 §2]都是研究的中心对象. 这四个构造都是无限维向量空间 [I.3 §2.3], 后两个还是 “代数”, 这意味着其中的元素不但可以相加, 可以与标量相乘, 还可以彼此相乘. 因为这些构造都是无限维的, 研究它们就要用到极限的论证, 这就是何以把它们都归入分析. 然而, C^*-代数和冯 · 诺依曼代数这些名词就表明在那些领域中也要本质地应用代数工具. 而 “空间” 一词就表示几何也会起重要的作用.

动力学 [IV.14]是分析的另一个引人注目的分支. 它研究的是: 当进行一个简单的过程, 而您又让它反复地一再进行下去, 那会发生什么? 例如, 取一个复数 z_0, 再令 $z_1 = z_0^2 + 2$, 然后是 $z_2 = z_1^2 + 2$, 并仿此以往, 那么, 序列 $z_0, z_1, z_2, \cdots$ 的极限性状如何? 它会一直走向无穷, 还是会停留在某个有界区域内? 结果是, 这个序列以一种复杂的方式依赖于原来的数 z_0. 它究竟如何依赖于 z_0, 这就是动力学的一个问题.

有时, 这个反复进行的过程是一个 “无穷小过程”. 举例来说, 已经给出了太阳系的各个行星在某一瞬间的位置和速度, 知道它们的质量 (还有太阳的质量), 这时

有一个简单的规则告诉您在以后的瞬间这些位置和速度将变成什么样. 后来, 既然位置和速度变了, 计算也就将改变; 但基本的规律仍然是一样的, 所以可以把整个过程看成是同一个简单的无穷小过程重复了无穷多次. 表述这件事的正确途径是利用常微分方程[①], 所以动力学的相当大一部分就是关于这些方程的解的渐近性态的研究.

2.6 逻辑

"逻辑" 这个词有时就是用作一种简写, 即所有关于数学本身的基本问题都算是逻辑, 其中值得关注的有集合理论 [Ⅳ.22]、范畴理论 [Ⅲ.8]、模型理论 [Ⅳ.23], 还有比较狭义的 "演绎的规则" 中的逻辑. 集合理论的成就中值得关注的有哥德尔的不完全性定理 [Ⅴ.15], 以及科恩 (Paul Cohen) 关于连续统假设的独立性的证明 [Ⅴ.18], 哥德尔定理对于数学的哲学理解有着戏剧性的作用. 虽然现在人们已经了解, 并非每一个数学命题都可以证明或反证, 绝大多数数学家还是和以往一样地行事, 因为他们所遇到的绝大多数命题倾向于是可判定的, 即可以证明的. 然而, 集合论专家却是另一类生灵. 从哥德尔和科恩以来, 又有许多其他命题被证明是不可判定的, 而且提出了许多新的公理来使它们成为可判定的. 这样, 可判定性的研究现在主要是为了数学的理由, 而不是为了哲学的理由.

范畴理论是另一个例子, 本来是来自研究数学的过程, 后来其自身也成了一个数学学科. 它与集合理论的不同在于: 它较少注意数学对象本身, 而是研究对这些对象做了什么事, 特别是关注把一个对象变为另一个对象的映射.

一组公理的模型就是这样一个数学结构, 使得这些公理在适当解释以后为真. 例如一个具体的群就是群的公理的一个模型. 集合论专家研究集合论公理的模型, 这些对于以上所述的著名定理的证明是很不可少的, 但是模型概念可以应用到更广的其他领域, 而且在相当远离集合论的地方导致了重要的发现.

2.7 组合学

可以试着用不同的方式来定义组合学. 每一种方式单独看都不能令人满意, 但是合起来却对这门学科是什么给出了一些概念. 第一种定义是: 组合学是讲的如何对事物计数. 例如, 可以用多少种不同方法用 1 和 0 来填满一个 $n\times n$ 正方形格网, 但要求每一行里最多有两个 1, 每一列里也最多有两个 1? 因为这个问题要求对一个什么东西进行计数, 所以它在简单的意义下是一个组合学问题.

组合学有时又称为 "离散数学", 因为它考虑的是 "离散的" 结构, 而不是 "连续的" 结构. 粗略地说, 说一个对象是离散的, 就是说它是由可以彼此分隔开来的点所构成的, 而说是连续的, 就是说, 可以从一个点移动到另一个点而不至于有突

① 原书作 "偏微分方程" 似乎不妥, 详见动力学 [Ⅳ.14]. —— 中译本注

然的跳跃 (离散结构的一个好例子是整数格网 $\mathbf{Z}^2$, 即平面上坐标为整数的点所成的格网, 球面则是连续结构的好例子). 组合学和理论计算机科学有密切的亲和关系 (后者从本质上说, 就是处理由 1 和 0 组成的序列的结构), 组合学有时也和分析对立起来讲, 虽然二者之间有一些联系.

对组合学的第三种观点是: 它处理的是具有 "极少" 限制的结构. 这个想法有助于解释以下事实: 尽管数论研究的是所有整数的集合, 这个清楚地是离散的集合 (当然还有别的), 可是数论并不被看成组合学的一个分支.

为了说明二者的上述对立, 现在有两个多少相似的问题, 它们都是关于正整数的:

(i) 是否存在一个可以用 1000 种不同方法写成平方和的正整数?

(ii) 设有正整数序列 $a_1, a_2, a_3, \cdots$, 且每一个 a_n 都位于 n^2 和 $(n+1)^2$ 之间, 是否存在一个正整数, 而可以用 1000 种不同的方式写成此序列中两数之和?

第一个问题是算作数论问题, 因为它考虑的是一个非常特定的序列 —— 完全平方数序列 —— 而希望用特定的数集合的性质来回答, 而答案是肯定的[①].

第二个问题则是关于一个构造要少得多的对象的. 关于 a_n, 我们只知道它的大略的大小 —— 它相当接近于 n^2 —— 但是对其更精确的性质, 例如是否素数, 是否完全立方数, 或是否 2 的幂, 则一无所知. 由于这个原因, 第二个问题属于组合学. 答案如何尚不得而知. 如果答案是肯定的, 则它在一定意义上表明, 第一个问题的数论的答案只是一个幻象, 真正起作用的只是完全平方序列的粗略的增长率.

2.8 理论计算机科学

这个数学分支将在第Ⅳ部分里详细讲述, 所以现在只简短地讲一下. 广泛地说, 理论计算机科学讲的是计算的效率问题, 就是为完成一定的计算任务所需的计算资源, 如计算机时间、存储量的大小等等. 有关于计算的数学模型, 使得能够很一般地研究计算效率问题, 而无需考虑算法如何具体执行. 这样, 理论计算机科学是纯粹数学的一个真正的分支, 从理论上说, 一个人可以是一个出色的理论计算机科学专家, 但不会为计算机编程. 然而, 它也有许多值得注意的应用, 特别是在密码学里 (详见*数学与密码* [Ⅶ.7]).

2.9 概率论

从生物学和经济学, 一直到计算机科学和物理学, 都有许多现象, 它们太复杂, 所以人们不是试图理解其全部细节, 而是提出概率性的命题. 例如, 如果您打算分

① 下面是一个快速的证明. 在*解析数论* [Ⅳ.2]这个条目开始处可以找到一个条件, 告诉您恰好是哪些数可以写为两个完全平方之和. 由此判据可知, "绝大多数" 整数不行. 仔细计数表明, 若 N 是一个大的整数, 则形如 m^2+n^2 的表达式, 其中 m^2, n^2 二者均小于 N, 这种表达式的个数比小于 $2N$, 且也可写为两个完全平方之和的表达式要多得多, 所以这里面一定有许多重复.

析一种疾病可能怎样传播, 您不会希望考虑到所有相关的信息 (例如谁和谁有了接触), 但是可以建立一个数学模型来分析它. 这种模型可能有想象不到的有趣的而且与实际工作有直接关联的性态. 例如, 可能有一个 "临界概率" p 存在, 它具有如下的性质: 如果在某类接触后受到感染的概率大于 p, 就可能发生传染, 而如果小于 p, 疾病就几乎一定会消失. 这样一种性态上的剧变称为相变 (进一步的知识可见临界现象的概率模型 [Ⅳ.25]).

2.10　数学物理

数学和物理学的关系几个世纪以来发生了深刻的变化. 直到 18 世纪为止, 数学与物理学之间并没有明确的区别, 许多著名的数学家同时也被看作是物理学家, 至少一部分时间被看作物理学家. 在 19 世纪和 20 世纪初, 情况逐渐发生变化. 到了 20 世纪中叶, 这两门学科已经相当地分离开来了. 然后, 到了 20 世纪末, 数学家们开始发现, 许多由物理学家发现的思想, 对于数学有着重大的意义.

这两门学科仍然有着巨大的文化上的差异: 数学家们对于寻找严格的证明兴趣要大得多; 而物理学家们则是把数学作为一种工具, 对于一个数学命题是否为真, 只要有了令人信服的论据, 哪怕这种论据还不真正就是一个证明, 物理学家也就满足了. 结果是, 物理学家是在不太严苛的限制下工作的, 所以, 他们时常远远早于数学家发现诱人的数学现象.

要找到支持这些发现的严格证明, 时常极为困难. 对于物理学家们没有认真怀疑过的命题, 要验证其真理性, 远不只是充满书生气的数学习题. 事实上, 它时常导致进一步的数学发现. 以下各个条目描述了数学和物理学怎样互相丰富了对方的诱人的例子. 这些条目有: 顶点算子代数 [Ⅳ.17]、镜面对称 [Ⅳ.16]、广义相对论和爱因斯坦方程 [Ⅳ.13]、算子代数 [Ⅳ.15].

I.2　数学的语言和语法

1. 引言

有一个值得注意的现象: 孩子们可以完全不必去管精巧的语法就能学会他们现在说的话. 其实, 成人也能从不去想什么词类、主语、谓语还有附属从句等等就能活得完全满意. 孩子和成人都能容易地辨别出不合语法的句子, 至少当语法错误不那么微妙时就行, 而且为此也不需要能够解释这些错误所违反的规则是什么. 然而, 毫无疑问的是, 如果有一点基本语法的知识, 就能大大促进对语言的理解. 而对于需要语言比较多的人, 比对于只需要不假思索地为了语言以外的目的而使用语言的人, 这种理解是不可少的.

关于数学语言也是这样. 到一定程度为止, 不必知道对他所用到的不同种类的

词如何分类, 也可以做数学、谈数学. 但是高深的数学里的许多句子都有着复杂的结构, 如果知道一点点数学语法的基本名词, 就容易懂得多. 这篇文章的目的就是解释最重要的数学"词类". 其中有一些和自然语言很相似, 有一些则大不相同. 正常情况下是在大学数学课程之始教这些东西的,《数学指南》的一大部分不需数学语法的准确知识也能懂得, 但是对于还想往下多读一点本书的比较高深部分的读者, 仔细读一下这个条目还是有帮助的.

需要使用数学语法的主要理由是, 数学命题是假设应该完全精确的, 而除非所用的语言没有通常的语言的许多含混与歧义, 完全精确是做不到的. 数学语句也可能是高度复杂的: 如果构成这些语句的各个部分不是清楚而且简单, 这些不清楚的地方就会很快地堆积起来, 使得整个句子无法理解.

为了说明数学的谈话所需要的清楚和简单, 我们来看一下一个著名的数学句子: "Two plus two equals four"[①](二加二等于四), 我们试图把它作为一个英语语句而不作为数学语句来进行语法的分析. 从表面上看, 它含有三个名词 ("two" "two" 和 "four")、一个动词 ("equals") 和一个连接词 ("plus"). 然而再细看一下, 我们就开始发现怪事了. 我们发现 "plus" 这个单词有点像英语单词 "and", 这是连接词的最明显的例子, 但是这两个单词的行径又颇不一样, 这一点可以从句子 "Mary and Peter love Paris"(马丽和彼得喜欢巴黎) 看出来. 在这个句子里, 动词 "love"(喜欢) 是用的复数形式, 后面没有加上 "s", 而在前一个句子里动词 "equals"(等于) 使用的是动词 "equal" 单数形式, 词尾加了 "s". 所以 "plus" 似乎是把两个对象 (现在恰好是两个数) 拿来做成了一个新的在英语语法上看成单数的对象, 而 "and" 则把 "Mary" 和 "Peter" 只是比较松散地连接在一起, 而仍是两个人, 所以后面的动词 "love" 要用复数形式了.

再多想一下 "and" 这个单词, 就发现它有两个很不相同的用法. 其一如上, 把两个名词连接起来, 另一种用法则是把两个句子连接起来, 例如 "Mary likes Paris and Peter likes New York"(马丽喜欢巴黎, 而彼得喜欢纽约). 如果要求我们的语言绝对清楚, 懂得这个区别就很重要 (当数学家达到最形式化的地步的时候, 他们就会取消 "and" 这个单词的连接名词的用法, 而 "3 and 5 are prime numbers"(3 和 5 都是素数) 这样的句子就要改写成 "3 is a prime number and 5 is a prime number" (3 是一个素数, 而 5 也是一个素数).

这只是许多类似问题之一: 随便哪个人想像标准的英语语法书那样把所有单词都分成八个标准的词类之一, 都知道这种分类是毫无希望地不够用的. 举例来说. 在 "This section has six subsections"(这一节有六个小节) 这样一个句子里, "six" 这

① 下面的分析涉及许多英语语法的概念, 尽管数学概念没有民族之分, 但从语法来说, 汉语和英语就大不相同. 为了能准确地表明原作的意思, 只好把原来的英语语句逐一照抄, 然后再试图译成汉语, 并加注解. 因此这里的文字也稍有修改. —— 中译本注

个词起的是什么作用？和前面的 "two"(二) 和 "four"(四) 不一样, 这里的 "six" 肯定不是名词. 因为它是修饰名词 "subsection" 的, 传统上是把它分类为形容词的, 但是它的行径又和绝大多数形容词不一样. "My car is not very fast"(我的车不很快) 和 "Look at that tall building"(看着那座高房子) 这两个句子完全符合语法, 但是下面两个句子: "My car is not very six" 和 "Look at that six building" 就不仅是毫无意思, 而且是不合语法的毫无意思. 那么, 我们是不是再把形容词细分为数字形容词和非数字形容词呢？说不定可以, 但是这样一来我们的麻烦还只是开了一个头. 像 "my"(我的) 和 "your"(你的) 这样的物主形容词又怎么办呢？[算数字形容词呢, 还是算非数字形容词呢？] 总起来说, 越想把英语单词的分类细化, 就越会认识到有多少种不同的语法功能.

2. 四个基本概念

另一个有着非常著名的三种不同意义的单词是 "is", 这三种意义可以用下面三个句子来说明:

(1) 5 is the square root of 25 (5 是 25 的平方根).

(2) 5 is less than 10 (5 比 10 小).

(3) 5 is a prime number (5 是一个素数).

在第一句里, "is" 可以用 "equals"(等于) 来代替, 它是说有两个对象, 即 5 和 25 的平方根, 二者事实上是同一个东西, 正如在英语的语句 "London is the capital of the United Kingdom"(伦敦是英国的首都) 里面的 "is"(是) 一样. 在第二个句子里, "is" 起着完全不同的作用. "less than 10"(<10) 这几个单词组成一个形容词短语, 表示一个数可能具有也可能不具有的性质, 而这个句子里的 "is" 正如英语句子 "Grass is green"(草是绿的) 里的 "is" 一样, 说明有这个性质. 至于第三个句子, 那里的 "is" 表示 "is an example of"(是其一例), 和英语的句子 "Mercury is a planet"(水星是个行星) 里的 "is" 一样.

"is" 的这三种不同的意义反映了一个事实, 即如果把这三句话用比较符号化的办法来表示, 它们就完全不一样了. (1) 的一个明显的写法是 $5 = \sqrt{25}$. 至于 (2), 通常会写为 $5 < 10$, 而 "<" 这个符号表示 "is less than"(比 …… 小). 第三个句子通常不用符号来写, 因为素数这个概念并不是那么基本, 所以没有一个普遍采用的符号与它相联系. 然而, 用符号来写, 有时还是有用的, 这就必须发明一个适当的符号. 办法之一是采用以下的规约, 即若 n 是一个正整数, 则 $P(n)$ 表示 "n 是一个素数". 使用集合的语言是另一种方法, 而其中并不隐藏 "is" 这个单词的其他用法.

2.1 集合

宽泛地说, 集合就是一些对象的集体, 或总体, 而在数学的论述里, 这些对象是

数学的对象, 如数、空间的点, 甚至是其他的集合. 如果我们要符号地重写 (3), 另一个方法是定义 P 为所有素数的总体, 即集合. 这样我们就可以把 (3) 重写为 "5 belongs to P"(5 属于集合 P). 属于某个集合这一概念是相当基本的, 值得为此专设一个符号, 而所用的符号即为 "$\in$". 所以 (3) 的完全符号化的写法就是 $5 \in P$.

集合的成员称为其元素, 而符号 "$\in$" 通常就读作 "is an element of"(是 ⋯⋯ 的元素). 这样, (3) 中的 "is" 与其说像 "=", 不如说更像 "$\in$". 虽然我们不能直接用 "is an element of" 这个短语来代替 "is", 但是若把句子的其余部分稍作修改, 则这种代替还是可以的.

有三种常用的方法来记一个特定的集合. 其一是把其所有的元素写在一个花括弧内, 例如 $\{2,3,5,7,11,13,17,19\}$ 就是共有 8 个元素 2, 3, 5, 7, 11, 13, 17, 以及 19 的集合. 数学家通常考虑的集合都太大 —— 甚至是无穷集合 —— 大到这样写行不通, 所以第二个写法就是用 ⋯⋯ 表示元素的清单太长, 写不下来, 例如 $\{1,2,3,\cdots,100\}$ 和 $\{2,4,6,8,\cdots\}$ 分别表示所有直到 100 为止的正整数的集合和正偶数的集合. 第三种, 也是最重要的一种方法是通过性质来定义集合, 下面的表达式就是这样做的一个例子: $\{x : x$ 是一素数, 而且 $x < 20\}$. 这样一个表达式的读法可以是: [先把冒号 ":" 读作 "使得"[①](或 "使得适合" "使得满足"); 接着读冒号后的文字; 最后读第一个花括号 "{" 后的元素记号并加上 "的集合", 所以现在的例子就读作 "使得适合 x 为一素数, 且 $x < 20$ 的 x 之集合"][②], 这个集合等于前面讲的集合 $\{2,3,5,7,11,13,17,19\}$.

数学里的许多语句都可以用集合的用语来重写. 例如, 句子 (2) 还可以重写为 $5 \in \{n : n < 10\}$. 这种做法时常没有什么意思 (例如, 现在写为 $5 < 10$ 要容易得多). 但是也有这样的情况, 使用集合的用语极为方便. 例如数学中一个大进展是用笛卡儿坐标来把几何翻译成代数, 其做法就是把几何对象定义为点的集合, 点则定义为一对实数, 或者实数的三元组. 这样, 例如集合 $\{(x,y) : x^2 + y^2 = 1\}$ 就是 (或者说 "就代表") 圆心在原点 $(0,0)$ 而半径为 1 的圆周. 这是因为由毕达哥拉斯定理, 从 $(0,0)$ 到 (x,y) 的距离是 $\sqrt{x^2+y^2}$, 这样, 句子 "$x^2 + y^2 = 1$" 就可以几何地重述为 "从 $(0,0)$ 到 (x,y) 的距离为 1". 如果我们关心的只是哪些点在此圆周上, 那么 "$x^2 + y^2 = 1$" 这样的句子也就可以勉强应付过去了, 但是在几何里, 时常需要把整个圆周看成单个的对象 (而不是许许多多的点, 也不是那些点所可能具有的性质), 这时, 集合论的语言就不可少了.

第二种没有集合就很难办的情况是在需要定义新的数学对象的时候. 很常见的情况是, 这个对象是一个附加了某种数学结构的集合, 这个结构的形状又是集合的元素间有某种关系. 集合论语言的这种用法的例子请参看条目一些基本的数学定

① 请参看序言第一段引用的罗素的话. —— 中译本注

② 方括号里的文字是中译本加的, 以下相同, 不再注明. —— 中译本注

义 [I.3]里关于数系和代数结构的 §1 和 §2.

在研究元数学 (metamathematics) 的时候, 集合时常是很有用的. 元数学的内容就是证明一些命题, 这些命题不是关于数学对象, 而是关于数学推理过程本身的. 这时, 如果能够设计一种很简单的语言 —— 词汇要小, 语法要不复杂 —— 使得能够, 至少在原则上能够把所有数学命题都翻译为这种语言, 就会大有帮助. 集合使我们能够大为减少所需的词类的数量, 把几乎所有的词都变成名词. 例如借助于元素属于的符号 "∈", 就可以除掉形容词, 例如前面就说过, 可以把 "5 is a prime number"(5 是一个素数, 这里素数的 "素" 字起形容词的作用①) 写成 "$5 \in P$". 这个过程当然有一点矫揉造作, 很不自然 —— 但是想一下把 "roses are red"(玫瑰是红的) 换成 "roses belong to the set R" 又如何? —— 但是, 在现在这样的前后文之下, 把形式语言变得既自然又易懂, 就并不重要了.

2.2　函数

我们现在把注意力从句子 (1)~(3) 的 "is" 转移到其他部分上来, 并首先集中注意于短语 "the square root of"(…… 的平方根). 如果我们想从语法上来思考这个短语的话, 首先就应该分析它在一个句子里起什么作用, 而这个分析是很简单的, 在事实上所有的有此短语出现的数学语句里, 它的后面一定会跟一个数的名称. 如果此数是 n, 就会产生出一个稍长的短语 "the square root of n"(n 的平方根), 它是一个名词短语, 表示一个数 (至少当此数是用作一个名词而非形容词时是如此). 举例说, 如果在句子 "5 is less than 7"(5 小于 7) 里, 把 "5" 换成 "the square root of 25", 就会得到一个新句子: "the square root of 25 is less than 7", 它仍然是一个语法上正确的句子 (而且为真).

数学上最基本的活动之一是取出一个数学对象, 再把它变换成另一个有时是同类的, 但有时又不是同类的数学对象. "the square root of" 把一个数变成数, 正如 "four plus"(加上四)、"two times"(乘上二)、"the cosine of", (…… 的余弦)、"the logarithm of"(…… 的对数) 一样. 非数值的例子则有 "the center of gravity of"(…… 的重心), 它把一个几何图形 (只要不是太奇怪, 或太复杂以至没有重心) 变成一个点 —— 这话的意思就是, 如果 S 代表一个图形, 则 "the center of gravity of S" 就表示一个点, 即 S 的重心. 粗略地说, 一个函数就是一个这样的数学变换.

把这个定义变得更加精确并不容易. 要问 "什么是函数" 就意味着要找出一个什么东西来作为答案, 但是函数似乎更像是一个过程. 此外, 当它们出现在一个数学语句里的时候, 它们的作为也不像是一个名词 (它们更像前置词, 虽然有一个确定的差别将在下一小节里讨论). 所以人们可以认为, 问 "the square root of" 是什么这个问题并不适当. 我们是否应该就满足于上面所作的语法分析呢?

① 关于形容词的另外的讨论, 请参看算术几何 [IV.5 §3.1].

事实却是：否. 在数学里, 一而再地会出现一个情况, 一个数学现象, 哪怕它可能很复杂, 很不像是一个 "东西", 但把它想作一个单个的对象又是很有用的. 我们已经看到了一个简单的例子：平面或空间里的无穷多个点的总体, 把它想作一个单个的几何形状, 有时会更好. 为什么人们对于函数也想这么做呢? 原因有二：首先, 能够说 "sin 的导数是 cos" 这样的话, 或者使用一般话语说某些函数是可微的, 而某些函数则不是, 这些情况下, 把函数看成一个 "东西" 都是很方便的. 更一般地说, 函数可以具有性质, 而为了讨论这些性质, 就更需要把函数看成一个 "东西". 其次, 许多代数结构, 看成函数的集合最为自然 (例如, 请看 [I.3 §2.1] 中关于群和对称的讨论, 又可见希尔伯特空间 [Ⅲ.37]、函数空间 [Ⅲ.29]以及向量空间 [I.3 §2.3]).

如果 f 是一个函数, 记号 $f(x)=y$ 表示 f 把对象 x 变成对象 y. 一旦一个人开始形式地来处理函数, 则准确地知道是对于哪些对象要让 f 去加以作用, 它们又能够变成哪样的对象, 就很重要了. 这样做的主要理由之一就在于, 这样就使得有可能讨论数学中的另外一个中心概念, 即函数的求逆 (为什么这是中心问题, 请见 [I.4 §1]). 粗略地说, 一个函数的逆, 就是能够消除此函数带来的变化的函数, 而且此函数也能消除其逆的作用. 例如把数 n 变成 $n-4$ 的函数, 就是那个把 n 变成 $n+4$ 的函数之逆, 既然先加了一个 4, 再减去这个 4, 或者逆向而行, 总能回到开始时的数.

下面是一个不可逆的函数. 它取每一个数, 并把它代之以最接近它的 100 的倍数, 而如果此数以 50 结尾, 则此函数把它进位. 这样, $f(113)=100, f(3879)=3900$, 而 $f(1050)=1100$. 显然, 不可能用一个函数 g 消除函数 f 的作用. 例如, 如果 g 能解除 f 对于数 113 的作用, 就应该令 $g(100)=113$. 但是同样的论证适合于每一个大到 50 为止同时又小于 150 的数, 而 $g(100)$ 不可能同时取多于一个值.

现在考虑把一个数加倍的函数, 它可以有逆吗? 可以的, 您会说除以 2 即可. 在绝大多数时间, 这个回答是完全合理的, 但是, 举例来说, 如果从上下文可以清楚看到, 所谈到的数都应是正整数的话, 这就不行. 那时, 需要集中注意于偶数和奇数的区别. 这个区别可以压缩为：所谓奇数就是那些使得方程 $2x=n$ 无解的数 (注意, 可以用减半来解除加倍过程. 这里的问题在于, 这两个过程是不对称的, 没有一个函数可以用加倍来解除, 因为加倍以后, 就再也回不到奇数上来).

因此, 要确定一个函数, 就必须同时仔细地确定两个集合：一个叫做 (定义) 域, 就是将被变换的对象的集合, 另一个叫 (值) 域, 就是那些变换以后的对象允许落入其内的集合. 一个由集合 A 到集合 B 内的函数, 就是一个规则, 使得可以按此规则对 A 中的每一个元素 x, 确定 B 中的元素 $y=f(x)$, 并不一定值域中的每一个元素都要被用到. 再一次考虑 "乘上 2" 这个例子, 它的定义域与值域都是正整数的集合. f 真正地可以取到的值的集合 $\{f(x):x\in A\}$ 叫做函数 f 的像 (这里有一点混淆, "像" 这个词也被用到 A 的单个元素 x 上：若 $x\in A$, 则它的像就是 $f(x)$).

下面的符号也会用到. 表达式 $f: A \to B$ 表示 f 是一个函数, 以 A 为定义域, B 为值域. 如果我们写出 $f(x) = y$, 我们就知道 x 一定在 A 中, 而 y 一定在 B 中. $f(x) = y$ 的另一个有时比较方便的写法是 $f: x \mapsto y$(箭头上加一短竖, 是为了与 $f: A \to B$ 中的箭头相区别, 后一个箭头的意义不同).

如果我们想要解除函数 $f: A \to B$ 的作用, 则只要能够避免前面讨论那个逼近函数时发生的问题, 我们就总能够解除其作用. 就是说, 只要当 x 和 x' 不同时, $f(x)$ 和 $f(x')$ 总不相同, 我们就能做到. 如果这个条件得到满足, f 就称为一个单射. 另一方面, 如果能够找到一个函数, 其作用能够被 f 所解除, 则只要能够避免在讨论整数加倍函数时遇到的情况, 这也总是可以做到的. 就是说, 只要对于 B 中的每一个元素 y, 都有 A 中某一个元素 x 使得 y 就是 $f(x)$, 就可以做到这一点 (这时, 我们可以选 $g(y) = x$ 来作出 g). 如果这个条件得到满足, 就说 f 是一个满射. 如果 f 既是单射又是满射, 就说 f 是一个双射. 双射就是有逆的函数.

重要的是要看到, 并非每一个函数都有干净的定义. 例如下面就确定了一个由正整数到正整数的函数: 若 n 为一素数, 就定义 $f(n) = n$; 若 n 的形式为 $n = 2^k$, 而 k 是一个大于 1 的整数, 则定义 $f(n) = k$. 对于其他的正整数 n, 都定义 $f(n) = 13$. 这是一个令人不快的随便写出来的函数, 但它是一个完全合法的函数. 事实上, "绝大多数" 函数, 虽然不是我们实际使用的绝大多数函数, 都是那么任意, 所以无法确定 (这些函数虽然作为个别的对象不一定有用, 但是需要有它们, 才使得从一个集合到另一个集合的所有函数的集合具有有趣的数学结构).

2.3 关系

现在我们来考虑句子 (2) 里的短语 "less than" 的语法. 和前面的 "the square root of" 一样, 它的后面必须跟一个数学对象 (现在的情况是必须跟一个数). 一旦做了这一点, 我们就又得到一个短语例如 "less than n", 但是它与 "the square root of n" 有重要的区别, 因为前者的作用类似于一个形容词而不如后者那样类似于名词, 但是它又是讲的性质, 而不是一个对象. 这一点恰好和英语里的前置词的行为类似, 请看英语句子 "the cat is under the table" 里的 "under".

因为数学的形式化的水平更高一些, 数学家们总是避免过多的词类, 我们在形容词的情况下就已经看到了这一点, 所以并没有一个符号来代替 "less than". 相反, 总是在它前面再加一个单词 "is", 成为 "is less than", 这样才用一个符号 "<" 来代替它. 这个符号的语法规则又是很简单的. 如果要在一个句子里使用符号 "<", 那么在它的前后各要放一个名词. 要想使这样得到的语法上正确的句子有意义, 这两个名词都应该代表数 (或者具有次序关系的更一般的数学对象). 一个如此行为的数学对象称为一个关系, 虽然称它为潜在的关系更加准确一些. "equals" 和 "is an element of" 是关系的另外两个例子.

和函数概念一样, 当确定一个关系时, 对于是讲哪些对象相关必须仔细一些. 通常, 一个关系总是与对象的一个集合 A 一起到来的, 是讲的 A 中的元素是有还是没有这种关系. 举例来说, 关系 "$<$" 可以定义在正整数的集合上, 也可以定义在所有实数的集合上. 在这两个情况下, 严格说来, "$<$" 代表不同的关系. 一个关系有时也可能是就两个集合 A 与 B 而言的. 例如, 若是讲的关系 "$\in$", 则 A 可以是所有正整数的集合, 而 B 可以说是所有正整数集合的集合.

在数学里有许多时候我们愿意把不同的对象看成是 "本质上相同" 的, 为了帮助把这个思想弄准确, 有一类非常重要的关系称为 "等价关系". 下面是两个例子. 第一个例子来自初等几何, 那里有时只关心形状, 而不关心大小. 两个图形, 若只需把反射、旋转、平移和放大组合起来, 就能把一个图形变为另一个图形, 就说这两个图形相似 (见图 1); "is similar to" 这个关系就是一个等价关系. 其次, 在做模算术 (准确一点应该称为同余算术)mod m[III.58] 时, 我们不想把相差 m 的倍数的两个整数加以区分, 这时我们就说这两个整数是同余 (mod$m$) 的. 关系 "is congruent (mod$m$) to"(mod$m$ 同余) 是另一个等价关系.

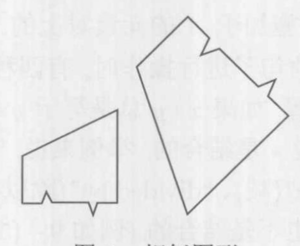


图 1 相似图形

这两个关系究竟有什么共同之处呢? 答案是: 它们都是取一个集合 (在第一个例子中是所有几何图形的集合, 而在第二个例子中是所有整数的集合), 并把它分裂为几个部分, 每一个部分各叫做一个等价类, 而同一个等价类内的各个元素就认为是 "本质上相同" 的. 在第一个例子里, 一个典型的等价类, 就是所有与某一个图形相似的图形; 而在第二个例子里, 则是在除以 m 后得到相同余数的整数的集合 (例如, 若取 $m = 7$, 有一个等价类就是 $\{\cdots, -16, -9, -2, 5, 12, 19, \cdots\}$).

等价关系另一个定义是, 一个定义在集合 A 上的关系 $\sim$ 称为等价关系, 如果它具有三个性质: 第一, 它是自反的, 意为对于 A 中所有元素 x 均有 $x \sim x$. 第二, 它是对称的, 意为若 x , y 均为 A 的元素, 而且 $x \sim y$, 则必有 $y \sim x$. 第三, 它是传递的, 意为若 x , y , z 都是 A 的元素, 而且 $x \sim y$, $y \sim z$, 则必有 $x \sim z$(想要对这些性质找到一点感觉, 可以看一下 "is similar to" 和 "is congruent to" 都有这三个性质, 而定义在正整数集合上的关系 "$<$", 虽然是传递的, 但非自反与对称的).

等价关系的主要用处之一是使得商 [I.3 §3.3]的构造这个概念精确.

2.4 二元运算

现在我们回到早前提出的例子："Two plus two equals four". 我们已经分析过其中的单词 "equals" 作为一个关系, 就是位于名词短语 "two plus two" 和另一个名词 "four" 之间, 并把它们连接起来成为一个句子. 但是 "plus" 又如何呢？它也是位于两个名词 "two" 之间. 然而其结果 "Two plus two" 并不是一个句子, 而是一个名词短语. 这种模式正是二元运算的特性. 二元运算的一些熟知的例子有 "plus"(加)、"minus"(减)、"times"(乘)、"divided by"(除以), 还有 "raised to the power"(乘方).

和函数一样, 我们惯于仔细注意二元运算施于其上的集合, 这样做会很方便. 从比较形式的观点看来, 集合 A 上的一个二元运算就是集合 A 上的一个函数, 它取出 A 中的一对元素, 而产生出再一个元素来. 更加形式一点, 二元运算就是一个函数, 它的定义域是所有元素对 $(x\ ,y)$(这里 x 和 y 是 A 的任意元素) 的集合, 而值域则是 A. 然而, 二元运算的记法并没有反映出这里提到的对于它的这种看法. 因为以 "plus" 为例, 我们总是记作 $x+y$, 好像这个运算是加在 A 的元素之上, 而按这里的说法, 二元运算是应该施加于 A 的元素对上的, 所以应该记作 $+(x,y)$[①].

在对含有一个二元运算的句子进行操作时, 有四种性质可能是很有用的. 用 $*$ 来记集合 A 上的任意二元运算. 如果 $x*y$ 总是等于 $y*x$, 就说 $*$ 是可交换的, 如果 $x*(y*z)$ 总等于 $(x*y)*z$, 就说 $*$ 是结合的. 举例来说, "plus" (加) 和 "times"(乘) 都是可交换与结合的, 而 "minus"(减)、"divided by"(除以) 和 "raised to the power"(乘到某次幂) 既不是可交换的, 也不是结合的 (例如 $9-(5-3)=7$, 而 $(9-5)-3=1$). 后几种运算提出了另一个问题：除非集合 A 选择得很仔细, 这几种运算可能没有定义. 例如, 如果限制只关注正整数, 则表达式 $3-5$ 就没有意义. 回应这一点, 可以想象到两个规定：其一是决定不再坚持一个二元运算要对 A 的每一对元素都有定义, 其二是把这一个二元运算处处有定义看成是一个让人喜欢的额外的性质. 然而, 真正实施的规定是：一个二元运算必须处处有定义, 所以 "minus" 虽然在所有整数的集合上是完全好的二元运算, 在所有正整数的集合上则不是一个二元运算.

如果对于 A 中的一切元 x, 集合 A 中的元素 e 都有 $e*x=x$, 就说它是 $*$ 的恒等元. 最明显的两个例子是 0 和 1, 它们分别是 "plus" 和 "times" 的恒等元. 最后, 如果 $*$ 有恒等元, 而 x 属于 A, 则 x 的逆元就是适合 $x*y=y*x=e$ 的 A 之元素 y. 例如, 若 $*$ 就是 "plus", 则 x 的逆元是 $-x$. 而若 $*$ 是 "times", 则 x 的逆元是 $1/x$.

二元运算的这些基本的性质对于抽象代数的各个结构是基本的. 详见**四个重要的代数结构** [I.3 §2].

---

① 这一句是译者改写的, 比原书更详细一些. —— 中译本注

3. 初等逻辑的若干知识

3.1 逻辑连词

逻辑连词是英语语法中连接词的数学等价物. 就是说, 它是一个单词 (或符号), 把两个句子连接起来成为一个新句子. 我们已经讨论过一个例子, 即 “and” 的连接句子的用法, 有时写为 “$\wedge$”(与), 特别是在比较形式或抽象的讨论里. 如果 P, Q 是两个命题 (请注意一个数学的习惯, 即不仅是数, 而且是任意对象, 都用一个字母来表示), 则 $P \wedge Q$ 也是一个命题, 而且它当且仅当 P, Q 二者均为真 [成立] 时才为真 [成立].

另一个逻辑连词是单词 “or”(或). 这个词对于数学家, 比对于通常说英语的人更有特定的意义, 它的数学用法可以用一个令人生厌的笑话来说明. [对于下面的问题: “Would you like your coffee with or without sugar?” (您的咖啡要或者不要加糖?) 回答 “yes, please”(就是 “随便, 加或不加都可以), 这里的 “或” 就是数学家的用法: 既可以加, 也可以不加, 并不是一定要排斥另一样, 如果您要加糖的, 就是不愿意不加糖, 反过来也是一样][1]. “或” 的符号, 如果您想用符号的话, 是 “$\vee$”, 而命题 $P \vee Q$ 为真 [成立], 只要 P 为真 [成立], 或者 Q 为真 [成立]. 这里也包括了二者同时为真 [成立][就是加或者不加糖都可以]. 所以数学家的 “或”, 是这个词的所谓包含性的用法.

第三个重要的连词是 “implies”(蕴含), 通常记作 “$\Rightarrow$”. 粗略地说, 命题 $P \Rightarrow Q$ 意味着 Q 是 P 的推论, 而且时常读作 “if P then Q”(若 P, 则 Q). 但是, 与 “or”(或) 的情况有点类似, 它在数学里和日常的英语语句中含义不太相同. 考虑下面比较极端的实例, 人们可能会认为它只是数学的迂腐, 但是它使您对数学语句和日常的英语语句的差别有一点感觉. 一次在吃晚饭的餐桌上, 我的小女儿说: “如果您是女孩子, 就把手举起来.” 我的一个儿子想逗她玩, 故意也举起手来, 因为她没有加上一句: “如果您是男孩, 就把手放下来”, 儿子的作为, [从数学上说] 与女儿的命令确实是符合的.

数学家对于 “implies”(蕴含) 的态度, 或者说对于 “if”(若、如果) 的态度, 有点和这个例子类似. 除了下面一种情况以外, 命题 $P \Rightarrow Q$ 都被认为是 “真 [成立]” 的, 就是只除去 “若 P 为真 [成立], 而 Q 不真 [不成立]” 一种情况, 只在这时, 才认为 $P \Rightarrow Q$ 不真 [不成立][2]. 这就是 “implies” 的 [按照数学家的用法的] 定义. [回到上面的例子, 令 P, Q 分别表示 “您是女孩” 和 “把手举起来”, 则唯一的被认为

---

[1] 方括号内的文字是译者改写的, 紧接的两个方括弧也是这个意思. —— 中译本注

[2] 本文时常用到 “真” 字, 这会有一点危险. 因为在日常生活里, 按作者的说法是在日常的英语语句里, 一件事, 或一个命题是否为真, 时常是按人的常识来判断的, 而在数学中则不是 (至少不一定是). 这里说的 “数学的蕴涵” 时常称为 “实质蕴含”(material implication). 把 “蕴含” 精确化为 “实质蕴含” 是逻辑学的一大进步. —— 中译本注

是违抗了这个指示, 即使得 $P \Rightarrow Q$ 不真 [不成立] 的情况是: "您是女孩, 但是又不举手"; "您是男孩"(即不是女孩) 但是也 "把手举起来" 了, 这并没有违抗女孩的指示]. "implies" 的这个定义有点混淆, 还因为在日常的英语里, "implies" 一词暗示在 P, Q 之间有某种联系, P 以某种方式导致了 Q, 至少是与它有关联. 如果是 P 为因, 导致了 Q 为果, 当然当 Q 不真时, P 也不可能真. 但是一个数学家关心的只是 P, Q 之间的逻辑推论关系, 而不是它们之间有什么因果关系, 或有什么 "理由". 所以, 如果需要证明 $P \Rightarrow Q$, 唯一要做的就是: 排除 P 为真 [成立] 而同时 Q 不真 [不成立] 的可能性. 现在给出一个例子: 若 n 为一正整数, 则命题 "n 为末位为 7 的完全平方数" 蕴含命题 "n 为素数", 这不是因为二者之间有什么联系, 而只是因为根本没有一个完全平方数末位为 7. 当然, 即使从数学上看, 那些更近乎真实的 "蕴含", 比之我们现在所讲的这种数学意义的蕴含, 也更有意思, 但是我们还是接受了数学的蕴含, 其原因仍然在于它避免了日常语言的某些歧义和细微的言外之意的差别.

3.2 量词

下面的古老的文字游戏使用了英语里的另一种含混之处, 使得我们必须从根本上重新考虑, 日常语言的用法和数学家的用法, 应以何者为更佳:

(4) Nothing is better than lifelong happiness (nothing 比终生的幸福更好).[①]

(5) But a cheese sandwich is better than nothing (但是, 吃一块奶酪三明治比吃 nothing 好, 即比什么都不吃好).

(6) Therefore, a cheese sandwich is better than lifelong happiness (所以, 一块奶酪三明治比终生的幸福更好).

我们现在来弄清楚这个文字游戏是怎么搞的 (这是拆穿一个笑话的好办法, 但是, 这个笑话有点像一个悲剧). 它的要点在于 "nothing" 这个单词, 它在这里是按两种不同意义来使用的. 在第一句里面, "nothing" 的意思是指 "终生的幸福" 比不论哪一件东西都好, "There is no single thing that is better than lifelong happiness."[说是 "nothing", 其实是说 "有一个什么东西", 是说的 "有"; 第二句的 "nothing" 则不然, 说的是: "吃一块奶酪三明治比什么都不吃" 好: "It is better to have a cheese sandwich than to have nothing at all", 这里的 "nothing" 是指 "什么都没有吃", 是说的 "没有"], (5) 里面的 "nothing" 就好比点了一份空菜单, 第一句里的 "nothing" 这样来解释就不成立了 (因为 "什么都没有吃" 并不比 "终生幸福" 更好).

诸如 "all"(所有的)、"some"(有一些)、"any"(任意一个)、"every"(每一个) 以及 "nothing"(没有一个) 这样一些单词, 都称为量词, 而在日常的英语语言里很容

① 这个笑话的关键就在于对于 "nothing" 怎样解释, 下文会详细分析这一点, 所以我们暂不译出 "nothing" 这个单词. —— 中译本注

易产生这一类歧义. 所以数学家们只用两个量词来应付过去, 而且使用的规则也要严格得多. 这些量词总是放在句首, 其一可以读作 “for all” 或 “for every”(对于所有的、对于一切、对于每一个等等), 另一个则读作 “there exists” (存在), 或 “for some”(对于某些) 等等. 句子 (4) 可以重写如下使它没有歧义 (但是也不像真正的英国话了):

(4′) For all x, lifelong happiness is better than x (对于所有的 x, 终生的幸福都比这个 x 更好).

第二个句子 (5) 则不能用这些单词来重写, 因为那里的单词 “nothing” 并不起量词的作用 (最接近于它的数学等价物, 是诸如空集 (即没有元素的集合) 之类的东西).

有了 “for all” 和 “there exists” 以后, 对于下面两个句子的起始部分的区别就可以看清楚了.

(7) Everybody likes at least one drink, namely water (每个人至少喜欢一种饮料, 就是水).

(8) Everybody likes at least one drink; I myself go for red wine (每个人至少喜欢一种饮料; 我就喜欢红酒).

第一句话是要论证 (虽然人们的证明并不一定对): 有一种饮料是人人都喜欢的, 而第二句则只是宣称: 各人各有所好的一种饮料, 这个 “一种饮料” 却可以因人而异. 把两句话的差别刻画出来的精确陈述如下:

(7′) There exists a drink D such that, for every person P, P likes D(存在一种饮料 D, 使得对于每一个人 P, P 都喜欢 D).

(8′) For every person P, there exists a drink D such that P likes D (对于每一个人 P, 都存在一种饮料 D, 使得 P 喜欢 D). ①

这里举例说明了一个重要的原则: 如果有一个句子, 它是这样开头的: “对于每一个 x, 存在一个 y, 使得 ······”, 把开头两小段调一个次序, 成为 “存在一个 y, 使得对于每一个 x ······”, 则将得到一个强得多的命题, 因为后一个句子里的 y 不再允许依赖于 x. 如果第二个命题仍然为真 [成立]—— 就是说, 可以确认选择一个 y, 同时适用于所有的 x—— 就说第一个命题一致地成立.②

常用 $\forall, \exists$ 这两个符号来分别表示 “for all” (对于所有的) 和 “there exists” (存在), 这将使我们, 只要愿意, 就能把很复杂的数学语句写成高度符号化的形式. 举例来说, 设用 P 表示所有素数的集合, 如我们前面做的那样. 这时, 以下的符号就是声称存在无穷多个素数, 或说是一个稍有不同的等价于它的声明.

① 请注意 (7′), (8′) 两个例句里的 “such that” (使得), 请比较序言第一段引用的罗素的话. —— 中译本注

② 这个说法显然是模仿数学分析里的一致连续、一致收敛等等而来的. —— 中译本注

(9) $\forall n\, \exists m, \quad (m > n) \wedge (m \in P)$.

用文字来写, 这就是说, 对于每一个 n, 都可以找到一个 m, 使得它既比 n 大, 又是一个素数. 如果我们还想把 (9) 进一步"解压", 还可以把其中的 $(m \in P)$ 这一部分写成

(10) $\forall a, b, \quad (ab = m) \Rightarrow ((a = 1) \vee (b = 1))$.

关于量词 "$\forall$" 和 "$\exists$", 最后还有一个重要的说明. 我们在讲它们时, 好像它们都是自立自主的, 但其实量词一定是和一个集合相关的 (就说这个量词取量于此集合上 (quantifies over the set)). 例如, 对于句子 (10), 如果 a, b 可以是分数, 此式就不能翻译成 "m 是素数", 例如, 如果 $a = 3, b = 7/3$, 则 $ab = 7$, 而 $a, b \neq 1$, 但这并不说明 7 不是素数. 一开始的符号 $\forall a, b$ 就已隐含了 a, b 应为正整数. 如果这一点不能从上下文看清楚, 我们就需要用到记号 $\mathbf{N}$(表示正整数集合), 并且把 (10) 的头改成 $\forall a, b \in \mathbf{N}$.

3.3 否定

在数学里, 否定的基本概念很简单: 有一个符号 "$\neg$" 代表 "否定"(not)[或者简单地称之为 "否""非"], 而如果 P 是任意数学命题, 则 $\neg P$ 就是这样一个命题: "当且仅当 P 不真 [不成立] 时, 它才为真 [成立]. "[换句话说, 若 P 为真 [成立], 则 $\neg P$ 不真 [不成立]; 若 P 不真 [不成立], 则 $\neg P$ 为真 [成立]]. 然而, 一个单词对于数学家的意义, 与对于普通人的意义相比, 要稍受限制, 这也是一个例子.

为了再一次说明这个现象, 我们取 A 为一个由正整数构成的集合, 并且问 "A 中每个数均为奇数" 这句话的否定是什么. 许多人在被问到这个问题是会回答说, 应是 "A 中的每个数均为偶数", 然而这是错的. 如果仔细想一想, 要使得第一个句子不真, 究竟需要什么, 那么就会看到, 需要的是 A 中至少一个数是偶数. 所以事实上, 这个句子的否定应是 "A 中存在一个数为偶数".

是什么原因使得会诱出第一个不正确的答案呢? 如果把这个句子更加形式化地写出来, 就看出产生错误的一种可能性了:

(11) $\forall n \in A$, n 为奇数.

如果只把这个句子的后半部分 "n 为奇数" 加以否定, 就得出了第一个答案, 但是我们要求的是整个句子的否定. 就是说, 我们要的并不是

(12) $\forall n \in A$, $\neg$(n 为奇数),

而是

(13) $\neg$($\forall n \in A$, n 为奇数),

而这等价于

(14) $\exists n \in A$, n 为偶数.

产生错误的第二个可能的解释是, (由于心理 — 语言学的原因) 人们倾向于把短语

"A 的每个元素" 看成是表示一个东西, 而它类似于 A 的典型单个元素. 如果有了一个特定的数 n 的感觉, 我们就会觉得 "n 为奇数" 的否定为 "n 为偶数". 补救的办法是把短语 "A 的每个元素" 看成自有其特殊本性的东西, 是一个较长的短语 "对于 A 的每个元素" 的缩写.

3.4 自由和约束变项

假设我们说这样的话: "抛射体在时刻 t 的速度是 v". 字母 t 和 v 代表实数, 而且称为变项, 因为在我们心里它们都是在变化着的. 更一般地, 一个变项则是用以代表一个数学对象的字母, 而不论它是否一个随时间变化的对象 [如果是随时间变化的量, 或者数, 或者函数, 就称为一个变量、变数, 甚至变元]①. 现在再来重看上面说正整数 m 为一素数的命题

(10) $\forall a, b, \quad (ab = m) \Rightarrow ((a = 1) \vee (b = 1))$.

在这个句子里有三个变项 a, b, m, 但是, 前两个和第三个在语法和语义上却有重要的区别. 这个区别造成了两个结果. 首先, 如果不事先已经从上下文知道了 m 是什么, 这个句子就实际上没有意义; 而重要的是, a 和 b 确实没有任何先验的意义. 其次, 问 "对 m 的哪些值, 句子 (10) 为真" 是完全有意义的; 但是要是问 "对于 a 的哪些值, 句子 (10) 为真" 就完全没有意义了. 句子 (10) 里的字母 m 代表一个在句子里未曾指明的定数, 而字母 a, b, 由于句子起始处的 $\forall a, b$, 就不再代表数 —— 而是以某种方式对于正整数对进行搜索, 试图找出一对正整数来, 使得其乘积等于 m. 这个差别的另一个表现是, 可以问 "m 是什么数", 但是不可以问 "a 是什么数". 第四个表现是, 如果在 (10) 中用别的字母代替 a 和 b, 句子的意义完全不受影响, 例如 (10) 也可以写成

(10′) $\forall c, d, \quad (cd = m) \Rightarrow ((c = 1) \vee (d = 1))$.

但是如果没有事先就确定了 n 表示和 m 同一的正整数, 就不能在 (10) 中把 m 换成 n. m 这样的变项称为自由变项, 可以这么说, 它好像是在那儿转来转去, 可以自由地取任意值. 像 a, b 那一类并不代表某一特定对象的变项称为约束变项, 或哑 (dummy) 变项 ("约束" 这个词主要是当变项出现在量词后面, 如句子 (10) 里那样, 才使用的).

一个变项是哑变项还有一个标志, 就是可以不用它们而改写它们出现于其中的句子. 例如表达式 $\sum_{n=1}^{100} f(n)$ 只不过是 $f(1) + f(2) + \cdots + f(100)$ 的简写, 在后一个写法里 n 根本没有出现, 所以在前一个写法里 n 其实什么也不代表. 要想实际消

① 这里最重要之点, 即 "variables" 可以没有物理的、几何的、"实际的" 背景. 在涉及逻辑的论述里, 它们可能就是一个逻辑的对象, 如命题、字母等等. 这时称为变项可能更加适当, 因为它不是数或量. 逻辑方面的著作里时常是这样做的. 在这个条目中, 只要涉及逻辑, 我们都会译为 "变项", 但在其他条目这则不一定如此苛求, 时常就说变量. —— 中译本注

除哑变项有时也做不到, 但是, 您感觉在原则上是可以做到的. 例如, "对于每个实数 x, x 或者为正, 或者为负, 或者为零" 这个句子, 多少有点像是把无穷多个这样的句子 "t 或者为正, 或者为负, 或者为零"(对应于每一个实数 t, 各有一个句子) 放在一起, 而每一个句子里都没有出现任何变项.

4. 形式化的程度

只需寥寥几个集合论的概念和逻辑名词, 就可以给出一种精确的语言, 它是那么多才多艺, 能够把通常的数学的所有命题都表示出来, 这实在令人吃惊! 有一些技巧需要整理出来, 但是, 如果不但允许以集合为基本对象, 还允许以数为基本对象, 连这也是可以避免的. 然而, 如果您去看一篇写得很好的数学论文, 则它的大部分并不是用的符号语言, 撒胡椒面似的撒一点 $\forall$, $\exists$ 之类, 而是用的像普通的英语 (有些论文是用别的语言写的, 特别是用法语, 但是英语已经成了数学的国际语言了). 数学家们怎么能够这么自信, 相信通常的英语不会导致混乱、歧义, 甚至错误?

答案在于, 数学家使用的语言典型地是一种认真推敲过的妥协物: 一方面是完全的口语化的英语, 它本会导致不可接受的不精确; 另一方面则是完全形式化的符号语言, 使人读起来像在做噩梦. 最理想的办法是用一种对读者友好的尽可能容易接受的语言来写作, 并且确信读者 (假设他们在阅读数学文章上都颇有经验, 受过训练) 在认为有必要的时候, 能够容易地使写的东西比较形式化. 这样做有时确实是必要的: 当一个论证很难掌握时, 使人确信这个论证为正确的唯一方法是更加形式地改写这个论证.

例如, 考虑数学归纳法 (许多证明都靠的是它) 的如下的重述:

(15) 每个非空的正整数集合都有一个最小的元素.

如果我们想把它翻译成更加形式化的语言, 就需要把诸如 "非空" "都有" 这些词语除掉. 但是这是很容易的. 想说某个正整数集合 A 非空, 简单地说存在一个属于 A 的正整数就行了. 这一点可以用符号写成

(16) $\exists n \in \mathbf{N}, n \in A$.

说 A 有一个最小的元素是什么意思? 这就是说, 存在一个元素 $x \in A$, 使得 A 中的每一个元素 y 要么大于 x, 要么等于 x 本身. 这又很容易地用符号写成

(17) $\exists x \in A, \quad \forall y \in A, \quad (y > x) \vee (y = x)$.

命题 (15) 说的就是 (16) 蕴含 (17), 所以就可以用符号写成

(18) $\forall A \subset \mathbf{N}$,

$$[(\exists n \in \mathbf{N},\ n \in A) \Rightarrow (\exists x \in A\,,\ \forall y \in A \quad (y > x) \vee (y = x))].$$

在这里, 同一个数学事实 (15) 就有了两种表示法. 显然, (15) 比 (18) 容易懂得多. 但是如果您关注的是数学基础, 或者打算写一个计算机程序来核查一个证明是否正确, 那么使用一个大为简化的语法和词汇就更好一些. 这时 (18) 就更加有利了. 在

实践上, 形式化有许多不同的程度, 数学家很善于在其中转换. 正是这一点才使得即令一个数学论证并没有写成 (18) 那样, 也能感到它完全可信 —— 当然, 这种转换也使得种种错误会成为漏网之鱼, 不时地钻了进来.

I.3 一些基本的数学定义

这一条目讨论的一些概念在现代数学的那么多地方都出现了, 所以, 等到第III部分再来讨论它们就不甚妥当了 —— 它们太基本了. 以后的许多条目都假设读者至少熟悉这些概念中的一部分, 所以, 如果您还没有见过这些概念, 读一读本文将大大帮助您理解本书.

1. 主要的数系

第一个展现在一个孩子面前的数学概念, 几乎总是数的概念. 这个概念一直停留在一切水平的数学的中心位置. 然而要想说明白 "数" 这个词的意义, 并不如初想的那么容易: 一个人数学学得越多, 就会见到这个词的更多的用法, 而对于数的概念也就变得更精巧. 这种个人对于数的认识的发展与多少个世纪的历史发展是平行的 (见*从数到数系*[II.1]).

现代关于数的观点是, 最好不要孤立地看待每一个数, 而把它看成一个较大的总体的一部分, 这种总体称为数系. 它们的突出的特点是可以在其上完成算术运算 —— 加、减、乘、除和开方. 关于数的这种观点是富有成果的, 它是通向抽象代数的跳板. 本节其余部分就是对于五种主要数系的简要描述.

1.1 自然数

自然数也叫正整数, 就是甚至小孩子都熟悉的那种数: $1, 2, 3, 4, \cdots$. 为了数学的最基本的目的 —— 计数 [就是 "数"(读三声) 数目, "数"(counting) 事物的个数]—— 使用的就是自然数. 自然数的集合通常用符号 $\mathbf{N}$ 来表示 (有些数学家愿意把 0 也归入自然数, 例如, 在逻辑学和集合理论中这是通常的规约, 但有的则否. 本书中两种规约都用, 但是要弄清楚, 用的究竟是哪一种规约).

当然, "$1, 2, 3, 4, \cdots$" 这样的短语不算是形式定义, 但是它确实建议了自然数的如下的基本图景, 我们在下面都以它为准:

(i) 给定一个自然数 n, 后面必紧跟着一个自然数 $n+1$, 称为 n 的后继者.

(ii) 如果一个自然数的单子从 1 开始, 而且每一个自然数以后都跟着其后继者, 则这个单子必定把每一个自然数都包括进来恰好一次, 而且不再包含其他东西.

这样一个图景被压缩成为*佩亚诺公理*[III. 67].

给定了两个自然数 m 和 n, 我们可以把它们相加和相乘, 在每个情况下都得

到一个新自然数. 与此相对照的是, 减法和除法就不一定总可能. 如果想使表达式 $8-13$ 或 $5/7$ 有意义, 就必须在一个更大的数系里面工作才行.

1.2 整数

自然数并不是仅有的完整而没有分裂开的数, 因为其中没有包括零和负整数, 这二者对于数学又是不可少的. 引入零的第一个理由是: 正整数的通常的十进位记数法需要它 —— 要是没有它怎能方便地写出 10057? 然而, 现在认为零的引入远非只是方便问题, 使得它值得注意的性质是: 它是一个加法恒等元, 就是说, 对任意数加上零都不改变原数. 虽然对一个数作一个不影响它的运算并无特别的意思, 这个性质本身却是很有趣的, 而且正是它, 使得零与其他数区别开来. 一个立即可得的例证是它使我们想到负数, 若 n 是一个正整数, $-n$ 的定义就是加到 n 上就会得到零的那个数.

一个几乎没有数学经验的人总会不假思索地认为数是用来计数的, 所以他们反对负数, 因为如果一个问题问的是 "有多少?" 则答案总不会是负数. 然而, 数的用途并非只是简单的计数, 许多情况都要以包括正数和负数的数系来做模型. 例如, 负数时常用来表示银行帐户里的存款. 温度 (华氏或摄氏度) 和距海平面的高度, 都有正负之分.

所有整数 —— 正负整数与零 —— 的集合时常记作 $\mathbf{Z}$(德文 "Zahlen"(数) 的第一个字母). 在这个数系里面, 减法总是可能的: 若 m 和 n 都是整数, 则 $m-n$ 也是.

1.3 有理数

迄今, 我们只考虑了完整的数. 如果我们再构造出所有的分数, 就得出了有理数. 所有有理数的集合记作 $\mathbf{Q}$(表示 "quotient", 商).

数的主要用途之一是 "量度", 而量度所得之量, 例如长度、重量、温度和速度, 绝大多数情况下都可以连续变化. 对于量度这样的量, 整数是不够用的.

有理数的重要性, 更加理论化的论证在于, 它们构成一个可以在其中进行除法的数系, 但是以零为除数作除法例外. 这个事实, 再加上算术运算的一些基本性质, 意味着 $\mathbf{Q}$ 是一个 "域". 域是什么, 为什么很重要, 将在后面 (§2.2) 详细解释.

1.4 实数

古希腊人的一个著名的发现 (这个发现常被归功于毕达哥拉斯学派, 虽然没有充分的证据 [VI.1]) 是: $\sqrt{2}$ 不是有理数. 就是说, 没有一个分数 p/q 可以使得 $(p/q)^2=2$. 关于直角三角形的毕达哥拉斯定理 (这个定理可能在毕达哥拉斯前至少 1000 年就已为人所知了) 告诉我们, 若以正方形的边长为 1, 则其对角线长为 $\sqrt{2}$. 这样, 存在一些不能用有理数来度量的长度.

这个论证似乎给出了进一步扩大数系的强有力的实际理由. 然而, 也可以拒绝这个实际理由: 说到底, 我们不能进行精确度为无限的量度, 在实际作量度时, 做到了一定的小数位数后, 就得舍入, 而只要我们这样舍入了, 就把量度的结果表示成有理数了 (这一点在条目**数值分析** [IV. 21]中将要更充分地讨论).

然而, 必须超越有理数系的理论论证是不能抗拒的. 如果我们要解多项式方程, 要取**对数**[III.25 §4], 要做三角, 或者要与**高斯分布**[III.71 §5] 打交道, 无理数就会处处出现了, 而这里还只是在无穷多的例子里举了四个. 无理数并不是直接为了量度之用, 但是当我们要对用数学描述的物理世界进行理论的推理时, 就用得着它们了. 这里必然使用了一些理想化: 如果要想对单位边长的正方形的对角线的长度作尽可能准确的量度, 那么, 说它是 $\sqrt{2}$, 就比讲述一通观测值到底是多少, 有多大的准确度, 这样做要方便得多.

实数系可以说是具有有限或无限十进小数展开式的数的集合. 在具有无限展开式的情况下, 实数不是直接定义的, 而是用一种逐步逼近的过程来定义的. 例如, 数 $1, 1.4, 1.41, 1.414, 1.4142, 1.41421, \cdots$ 的平方, 可以如您所要求的那样接近 2, 只要在这个序列中走得足够远就行了. 我们说 2 的平方根是 $1.41421\cdots$ 的意思就是这样.

实数的集合记作 $\mathbf{R}$. 对于 $\mathbf{R}$, 一个较抽象的看法是: 它是有理数系扩充为一个更大的域, 而且, 再进行上述的过程, 仍然只能得到 $\mathbf{R}$ 中的数 [再不会得到更新的"数" 了].

由于实数与 (逐步逼近的) 极限紧密的联系着, 对实数系真正的领会就依赖于对数学分析的理解. 数学分析将在 §5 里面讨论.

1.5 复数

许多多项式方程, 例如 $x^2 = 2$, 虽然没有有理数解, 却可以在 $\mathbf{R}$ 中解出. 但是还有许多这样的方程在 $\mathbf{R}$ 中也不能解出. 最简单的例子就是方程 $x^2 = -1$, 它没有实解, 因为所有实数的平方要么为正, 要么为零. 为了绕过这个问题, 数学家们引进了一个符号 i, 而且还简单地规定 i^2 要看成 -1. 复数系记作 $\mathbf{C}$, 就是形如 $a + b\mathrm{i}$ 的数的集合, 这里 a 和 b 是实数. 要把复数相加或相乘, 只要把 i 当成一个变元一样 (如同 x 一样), 但是, 只要一见到 i^2, 就把它换成 -1 . 所以

$$(a + b\mathrm{i}) + (c + d\mathrm{i}) = (a + c) + (b + d)\mathrm{i},$$

还有

$$\begin{aligned}(a + b\mathrm{i})(c + d\mathrm{i}) &= ac + bc\mathrm{i} + ad\mathrm{i} + bd\mathrm{i}^2 \\ &= (ac - bd) + (bc + ad)\mathrm{i}.\end{aligned}$$

关于这个定义有几点需要说明. 首先, 尽管它看起来似乎是人特意造出来的, 却不会引起任何不相容的矛盾. 其次, 虽然复数并没有对任意的事物进行计数或量

度, 它们却有极广泛的用处. 最后, 也可能是最令人吃惊的是, 虽然 i 的引进只是帮助我们求解恰好一个方程 $x^2+1=0$, 它却允许我们解出所有的多项式方程. 这就是著名的代数的基本定理 [V.13].

复数有这么大的用处有一种解释, 那就是它们通过阿尔干图示 (Argand diangram), 提供了一种简明的方式来讨论几何学的许多方面. 这种图示把复数表示为平面上的点, 数 $a+b\mathrm{i}$ 相应于坐标为 (a,b) 的点. 若 $r=\sqrt{a^2+b^2}, \theta=\arctan(b/a)$, 则 $a=r\cos\theta, b=r\sin\theta$. 结果用 $a+b\mathrm{i}$ 去乘复数 $z=x+y\mathrm{i}$ 就相应于下面的几何步骤: 首先把 z 和平面上的点 (x,y) 对应起来. 其次用 r 去乘这个点, 得到点 (rx,ry). 最后再把这个新点绕原点旋转一个角 $\theta(\theta\geqslant 0$ 时, 就作逆时针旋转 θ; $\theta<0$ 时则顺时针旋转一个角度 $-\theta)$. 换句话说, 乘以复数 $a+b\mathrm{i}$ 的效果就是: 按比例 r 放大, 再旋转一个角 θ. 特别是, 如果 $a^2+b^2=1$, 则乘以复数 $a+b\mathrm{i}$ 就相应于旋转一个角 θ.

由于这个原因, 为了表示复数, 极坐标至少和笛卡儿坐标一样好. 另一个表示复数 $a+b\mathrm{i}$ 的方法是把它写成 $r\mathrm{e}^{\mathrm{i}\theta}$, 这个式子告诉我们, 这一点离原点的距离是 r, 而且位于与正实轴成角度 θ 的方位上 ($\theta\geqslant 0$ 时, 方位角按逆时针方向计; $\theta<0$ 时, 则按顺时针方向的 $-\theta$ 来计). 若 $z=r\mathrm{e}^{\mathrm{i}\theta}$ 且 $r>0$, 则称 r 为 z 的模, 记作 $|z|$, θ 则称为 z 的幅角 (因为对 θ 增加 2π 并不会改变 $\mathrm{e}^{\mathrm{i}\theta}$, 通常都认为 $0\leqslant\theta<2\pi$, 但有时也规定 $-\pi\leqslant\theta<\pi$). 最后还有一个有用的定义: 若 $z=x+y\mathrm{i}$ 是一个复数, 则其共轭复数记作 $\bar{z}$, 就是复数 $x-y\mathrm{i}$. 容易验证, $z\bar{z}=x^2+y^2=|z|^2$.

2. 四个重要的代数结构

前一节里我们强调了: 数, 最好是不看成个别的对象, 而是看作数系的元素. 数系里面包含了一些对象 (即数), 以及施加于它们的一些运算 (如加法和乘法). 这样, 数系就是一个代数结构. 然而, 还有许多不是数系的重要的代数结构, 这里就要介绍其中的一些.

2.1 群

若 S 是一个几何图形, S 上的一个所谓刚性运动, 就是一种移动 S 的方式, 使得在此运动中, S 的任意两点的距离不变 —— 就是不允许挤压和拉伸. 如果在一个刚性运动以后, S 的形状不变, 就说这个刚性运动是 S 的一个对称. 举例来说, 设 S 是一个等边三角形, 让 S 绕它的中心旋转 $120°$, 这个旋转就是一个对称; S 对于经过其一个顶点与该点对边中点的直线作反射, 这也是一个对称.

更形式地说, S 的一个对称就是一个由 S 到其自身的函数 f, 使得 S 的任意两点 x 与 y 的距离与变换后的两点 $f(x)$ 与 $f(y)$ 的距离相同.

这个思想可以大大地推广: 如果 S 是任意的数学结构, S 的对称就是一个由

S 到其自身的保持这个结构的函数. 如果 S 是一个几何图形, 则应该得到保持的数学结构就是其任意两点的距离. 但是还有许多其他的数学结构会要求这个函数去保持, 其中最值得注意的是下面就要讨论的那一类代数结构. 与这里讲的几何情况作一个类比, 并且把任意的保持结构的函数都看成某种对称, 这样做是富有成果的.

由于有这样的极端的广泛性, 对称在数学里面就是一个渗透到各处的概念: 只要哪里有了对称出现, 群的概念就会紧紧地跟上来. 为了解释群是什么, 它们又为什么会紧紧跟上来, 让我们回到等边三角形的例子, 将会看到它恰好有六个可能的对称.

为什么会这样? 令 f 是顶点为 A, B, C 的等边三角形, 而且为简单计, 设它的边长为 1. 这时, $f(A), f(B), f(C)$ 就是此三角形中的三个点, 而其彼此的距离都必定是 1. 由此可知 $f(A), f(B), f(C)$ 必是此三角形的不同的顶点, 因为这个三角形中任意两点的距离最远只能是 1. 这样, 它们只不过是 A, B, C 三点重排了次序. 但是 A, B, C 的次序只可能有 6 个. 不难看到, 一旦选定了 $f(A), f(B), f(C)$, 则三角形内任意点处 f 的值也就完全确定了 (例如, 设 X 是 A, C 两点的中点, $f(X)$ 也就一定是 $f(A)$ 和 $f(C)$ 的中点, 因为再没有其他的点到这两点的距离分别是 1/2).

让我们写出 A, B, C 三点在变换以后的次序, 由此来记这些对称. 所以, 举例来说, 对称 ACB 就是保持 A 点不动, 而令 B, C 交换位置的对称, 只要把三角形对于过 A 和 B, C 中点的连线作反射, 就可以得到这个对称. 一共有 3 个这样的对称: ACB, CBA, BAC, 还有两个旋转 BCA, CAB. 最后还有一个 "平凡的" 对称 ABC, 它让所有的点都不动 (这个 "平凡的" 对称的用处, 恰好和零在整数加法的代数里的作用一样).

使得对称的这一个集合以及其他的集合成为群的, 是任意两个对称可以互相复合, 意思是一个对称以后再跟着一个对称就会产生第三个对称 (因为如果两个运算都能保持一个结构, 它们的复合很清楚也是这样), 例如, 如果在反射 BAC 后面再来一个反射 ACB, 就会得到一个旋转 CAB. 要看出这件事, 我们或者可以画一个图, 或者用以下的推理: 第一个对称把 A 变成 B, 第二个对称又把 B 变成 C, 所以它们的复合就把 A 变成 C, 类似地, 也就把 B 变成 A, C 变成 B. 但是注意, 进行对称的次序是有关系的: 如果是先作反射 ACB, 再作 BAC, 就会得到旋转 BCA(如果打算用画图来确定这一点, 记住把 A, B, C 看成标记顶点可能占据的位置的标签, 而不要让它们也随三角形运动).

我们把对称本身也看成 "对象". 而把复合看成是对于这些对象的代数运算, 有点像加法和乘法之于数一样. 这个运算有下面的有用的性质: 它是结合的, 平凡对称是恒等元, 而每一个对称都有逆[I.2 §2.4](例如, 每一个反射的逆就是它自身, 因为同一个反射作两次会使得三角形不动). 更一般地说, 任何一个带有一个二元运算

的集合, 若此运算有以上的性质, 就叫做一个群. 至于这个运算是否可交换, 这并不是群的定义的一部分, 因为如我们刚才所看见的, 复合两个对称时, 哪一个在先, 哪一个在后是有区别的. 然而, 如果这个二元运算是可交换的, 这个群就成为阿贝尔群, 取这个名词是为了纪念挪威数学家阿贝尔[VI.33]. 数系 $\mathbf{Z}, \mathbf{Q}, \mathbf{R}, \mathbf{C}$ 对于加法都是阿贝尔群, 或者用我们常用的说法, 它们在加法下成为阿贝尔群. 如果把零从 $\mathbf{Q}, \mathbf{R}, \mathbf{C}$ 中除去, 它们在乘法下也是阿贝尔群, 但是 $\mathbf{Z}$ 并不是, 因为缺少逆元: 整数的倒数, 一般并不是整数. 本条目后面还会讲群的其他例子.

2.2 域

虽然好几个数域都是群, 但是只把它们看成群就是忽略了其代数结构的很大一部分. 特别是, 群里面只有一个二元运算, 标准的数系却有两个, 即加法和乘法 (由此还可以得到其他附加的运算, 如减法和除法). 域的形式定义很长, 它是一个具有两个二元运算的集合, 还有几个这些运算必须满足的公理. 幸运的是, 有一个好办法来记忆这些公理. 先把数系 $\mathbf{Q}, \mathbf{R}$ 和 $\mathbf{C}$ 中的加法和乘法所满足的性质写出来.

这些性质如下. 加法和乘法都是可交换的以及结合的, 二者都有恒等元 (对于加法是 0, 对于乘法是 1). 每个元素 x 都有加法逆 $-x$ 和乘法逆 $1/x$(但是 0 没有乘法逆). 正是由于这些逆元的存在, 使得我们能够定义减法和除法: $x-y$ 意思就是 $x+(-y)$, 而 x/y 则是 $x\cdot(1/y)$.

这就覆盖了加法和乘法单独具有的全部性质. 但是在定义数学结构时, 有一个很一般的原理: 如果一个数学定义可以分成几个部分, 则除非这些部分可以相互作用, 否则这个定义是没有什么意思的. 现在加法和乘法就是这两个部分, 而迄今所讲到的性质并未把它们以某种方式连接起来. 但是最后还有一个性质, 即分配律, 做到了这一点, 从而完成了对于域的性质的刻画. 这就是把括号乘开来的规则: 对于域中的任意三个元 x, y 和 z, 有 $x(y+z)=xy+xz$.

在列出了这些性质以后, 可以抽象地来看待整个情况, 并把这些性质看作公理, 于是我们说: 域就是具有两种二元运算的集合, 这些运算需适合以上全部公理. 但是, 当我们在域中从事工作时, 通常并不是把这些性质看成公理的清单, 而是看作一个许可证: 允许我们在其中做有理数域、实数域和复数域中的所有代数运算.

很清楚, 公理越多, 寻找满足它们的数学结构就越难, 而且真的, 遇到域的情况比遇到群的情况更少见一些. 因此, 理解域的最好的办法可能莫过于集中注意于例子. 除了 $\mathbf{Q}, \mathbf{R}$ 和 $\mathbf{C}$ 以外还有一个域跳了出来, 成为域的一个基本的例子, 它就是整数 mod$p$(这里 p 是一个素数) 所成的集合 $\mathcal{F}_p$, 其中的加法和乘法都是 mod p 来定义的 (见模算术[III.58]).

使得域有意义的其实还不在于存在这些基本的例子, 而在于有一个重要的过程与域有关, 这个过程称为域的扩张, 它使我们能够从原来的域构造出新的域来. 这

里的思想是：先已有了一个域 $\mathcal{F}$, 找一个多项式 P 使它的根不在 $\mathcal{F}$ 中, 然后把一个新的元素“附加”到 $\mathcal{F}$ 上, 规定这个新元素是 P 的不在 $\mathcal{F}$ 中的根 [用这个根和 $\mathcal{F}$ 中的元素通过一切可能的加法和乘法做出新的式子来, 这些式子就构成了一个新的域 $\mathcal{F}'$. 称为 $\mathcal{F}$ 的扩张].

我们已经见到过域 $\mathbf{R}$ 的扩张过程的一个例子. 多项式 $P(x)=x^2+1$ 在 $\mathbf{R}$ 中没有根, 于是我们把 i 附加到 $\mathbf{R}$ 上去, 得到了所有形如 $a+b\mathrm{i},(a,b\in\mathbf{R})$ 的式子, 这样就得到了复数域 $\mathbf{C}$.

我们也可以把恰好就是这个过程用于 $\mathcal{F}_3$, $P(x)=x^2+1$ 在其中也没有根. 如果我们这样做了, 也会得到一个新的域, 它和 $\mathbf{C}$ 一样, 也是形如 $a+b\mathrm{i}$ 的复合所成的一个集合, 但是现在的 a 和 b 都是 $\mathcal{F}_3$ 的元素. 因为 $\mathcal{F}_3$ 中只有 3 个元, 所以现在的新域只有 9 个元素. 再一个例子是 $\mathbf{Q}(\sqrt{2})$, 它是 $a+b\sqrt{2}$ 这样的数的集合, 这里 a 和 b 是有理数. $\mathbf{Q}(\gamma)$ 是一个稍微复杂的例子, 这里 γ 是多项式 x^3-x-1 的根. 这个域的典型的元素就是形如 $a+b\gamma+c\gamma^2$ 的式子, 而 a,b 和 c 是有理数. 如果我们在 $\mathbf{Q}(\gamma)$ 中做算术, 则见到 γ^3 就要把它换成 $\gamma+1$(因为 $\gamma^3-\gamma-1=0$), 正如在复数域中见到 i^2 就要换成 -1 一样. 为什么域的扩张很重要, 更详细的讨论可见本条目 §4.1 的自同构.

引进域的第二个非常值得注意的根据在于它们可以用来构成向量空间. 下面就来讲向量空间.

2.3 向量空间

在一个向各个方向都伸展到无限远处的平面上代表一个点的最方便的方法之一是使用笛卡儿坐标. 选一个原点以及两个通常选为互相成直角的方向 X,Y. 如果从原点出发, 沿方向 X 走过距离 a, 再从这一点继续沿方向 Y 走过距离 b, 那么 (a,b) 这一对数就表示所达到的平面上的点 (如果 a 是一个负数, 如 -2, 就表示在 X 的反方向上走 $+2$, 对 b 也类似).

同是这件事换一个说法是：令 x 和 y 表示 X 和 Y 方向的单位向量, 它们的笛卡儿坐标分别是 $(1,0)$ 和 $(0,1)$. 这时, 平面上的每一个点都是基底向量 x 和 y 的线性组合 $ax+by$. 为了解释 $ax+by$ 这个表达式, 先把它写成 $a(1,0)+b(0,1)$. 用 a 乘单位向量 $(1,0)$ 得到 $(a,0)$, 再用 b 乘单位向量 $(0,1)$ 得到向量 $(0,b)$. 把 $(a,0)$ 和 $(0,b)$ 按坐标相加就得到向量 (a,b).

下面是线性组合出现的另一个情况. 设给了一个 [线性] 微分方程 $(\mathrm{d}^2y/\mathrm{d}x^2)+y=0$, 而又知道了 (或者注意到了)$y=\sin x$ 和 $y=\cos x$ 是两个可能的解, 则容易验证, 对于任意的数 a 和 b, $y=a\sin x+b\cos x$ 也是解. 就是说, 已经存在的解 $\sin x$ 和 $\cos x$ 的任意线性组合仍然是解. 结果会得出, 所有的解都是这种形式, 所以我们把 $\sin x$ 和 $\cos x$ 也看成这个 [线性] 微分方程的解“空间”的“基底向量”.

线性组合出现在整个数学的许许多多的情况下. 再给一个例子, 任意的 3 次多项式的形状都是 ax^3+bx^2+cx+d, 它是四个基底多项式 $1,x,x^2,x^3$ 的线性组合.

向量空间就是一个线性组合概念在其中有意义的数学结构. 属于此向量空间的对象, 除非我们在讨论一个特定的例子, 或者把它想作一个具体的对象, 如多项式或 [线性] 微分方程的解的时候, 通常就称为向量. 稍微形式化一点, 一个向量空间就是一个集合 V, 使得对其中任意两个向量 (即 V 的元素)v 和 w, 以及任意两个实数 a 和 b, 都可以构成其线性组合 $av+bw$.

注意, 线性组合涉及两个不同类的对象, 一类是向量 v 和 w, 另一类是数 a 和 b. 后者称为标量. 构造线性组合的运算可以分成两个组成部分, 即加法以及乘以标量. 为了构造出 $av+bw$, 先要用标量 a 和 b 去乘向量 v 和 w, 分别得出向量 av 和 bw, 再把所得的向量加起来, 得出完全的线性组合 $av+bw$.

线性组合的定义必须服从一些自然的规则. 下列的相加要是可交换的和结合的, 就有恒等元 (称为零向量). 对于每一个向量 v, 又必须有逆元 (记作 $-v$). 乘以标量也要服从某种结合律, 即 $a(bv),(ab)v$ 必须恒相等. 我们也需要两个分配律, 即对任意的标量 a,b 和任意的向量 v,w 均有 $(a+b)v=av+bv$, 以及 $a(v+w)=av+aw$.

还有一个线性组合会出现的数学情景, 而且这个情景又位于向量空间之所以有用的心脏位置, 这就是联立的 [线性] 方程的求解. 设给了两个 [线性] 方程 $3x+2y=6, x-y=7$. 求解这一对 [线性] 方程的通常的方法是设法消去 x 或 y, 办法是把一个方程的适当的倍数加到另一个方程上去, 也就是作这两个方程的某个线性组合. 现在, 我们可以把第二个方程的 2 倍加到第一个方程上去, 这样得到等式 $5x=20$, 而它告诉我们 $x=4$, 从而 $y=-3$. 为什么允许我们把两个方程像这样组合起来? 让我们把第一个方程的左右双方分别记作 L_1 和 R_1, 第二个方程的左右双方则记作 L_2 和 R_2, 于是有 $L_1=R_1, L_2=R_2$, 由此可以清楚地看到 $L_1+2L_2=R_1+2R_2$, 因为这个等式的双方其实是相同的数, 不过用了不同的记号罢了.

给定了一个向量空间 V 以后, 所谓它的基底无非就是具有以下性质的一组向量: $v_1,v_2,\cdots,v_n$, 而 V 的任意元素, 即任意向量都可以用唯一的方式写成它们的一个线性组合 $a_1v_1+a_2v_2+\cdots+a_nv_n$. 可能有两种情况使得这件事失败: 一是可能有某个向量不能写成 $v_1,v_2,\cdots,v_n$ 的线性组合, 二是可能有一个向量虽然可以写成这种线性组合, 但是写法不止一种. 如果 V 的所有向量都可以写成 $v_1,v_2,\cdots,v_n$ 的线性组合, 就说 $v_1,v_2,\cdots,v_n$ 张成了整个空间 V. 如果没有哪一个向量能以多于一种方式写成它们的线性组合, 就说 $v_1,v_2,\cdots,v_n$ 是独立的. 一个等价的定义是: $v_1,v_2,\cdots,v_n$ 是独立的, 如果把零向量写成 $a_1v_1+a_2v_2+\cdots+a_nv_n$ 的方法只能是取 $a_1=a_2=\cdots=a_n=0$.

基底中元素的个数称为 V 的维数 (或简称维). 一个向量空间不会有两个大小不同的基底, 这一点并非显然, 但是可以证明确实不会有, 所以维的概念才有意义.

对于平面, 前面说到的向量 x 和 y 构成了一个基底, 所以平面的维数是 2, 正如我们希望的那样. 如果取两个以上的 [平面] 向量, 它们不会是独立的. 例如取 3 个向量: $(1,2),(1,3)$ 和 $(3,1)$, 则可以把 $(0,0)$ 写成 $8(1,2)-5(1,3)-(3,1)$(想要把这一点做出来, 必须要解出一个联立 [线性] 方程组, 而在向量空间里, 这是典型的计算).

最明显的 n 维向量空间就是由 n 个实数所成的序列 $(x_1,x_2,\cdots,x_n)$ 的空间. 如果要把序列 $(y_1,y_2,\cdots,y_n)$ 加到它上面去, 只需构造序列 $(x_1+y_1,x_2+y_2,\cdots,x_n+y_n)$ 即可, 要用标量 c 去乘它, 只需作 $(cx_1,cx_2,\cdots,cx_n)$ 即可, 这个向量空间记作 $\mathbf{R}^n$. 所以具有通常的坐标系的平面是 $\mathbf{R}^2$, 而 3 维空间则是 $\mathbf{R}^3$.

基底中的向量的个数并不一定是有限数. 一个没有有限基底的向量空间称为无限维的. 这并不是一个奇怪的性质, 许多最重要的向量空间, 特别是"向量"为函数的向量空间, 常是无限维的.

关于标量, 还有最后一个说明. 在前面标量是定义为构造向量的线性组合时所用的实数. 但是结果是, 我们对标量所做的计算, 特别是在解联立方程时所做的计算, 在更广泛的前后文关系下也可以做. 真正重要的是它们必须属于一个域, 所以 $\mathbf{Q},\mathbf{R}$ 和 $\mathbf{C}$ 都可以用作标量的系统, 说真的, 更一般的域也是可以的. 如果一个向量空间 V 的标量来自域 F, 就说 V 是域 F 上的向量空间. 这个推广重要而且有用, 例如可见代数数[IV.1 §17].

2.4 环

另一个非常重要的代数结构是环. 环对于数学并不如群、域或向量空间那样处于中心地位, 所以适当的讨论要推迟到条目环, 理想与模[III.81] 中. 然而粗略地说, 环就是具有域的几乎所有的但不是所有性质的代数结构. 特别是对于乘法运算, 环就不如域要求得那么严格, 最重要的放松之处是, 不要求环中的非零元具有乘法逆, 而且有时环的乘法不一定是可交换的. 如果它是, 这个环就叫做可换环 —— 可换环的典型例子就是所有整数的集合 $\mathbf{Z}$, 另一个例子是系数在某个域 F 中的多项式的集合.

3. 从老结构产生出新结构

要理解一个数学结构的定义, 重要的第一步是找到足够多的例子. 一个定义, 如果没有例子, 就会是枯燥而抽象的. 有了例子, 就开始找到了对于这个结构的感觉, 而仅仅定义是提供不了这种感觉的.

造成这种情况的理由之一是, 例子使得回答基本问题要容易得多. 如果关于某个给定类型的结构有了一个一般的命题, 又想知道它是否正确, 这时, 如果能够在范围很广的特殊情况下去检验这个命题, 那会是很有帮助的. 如果这个命题通过了所有的检验, 就有了有利于这个命题的证据. 如果您还有好运气, 还可能看出, 这个

命题为什么是正确的; 反过来, 也可能发现这个命题对于您试验的每一个例子都是对的, 但是都是由于这些作检验用的例子本身有特别之处. 这时就会知道, 如果想找一个反例, 就应该避免这些特别之处. 如果确实找到了一个反例, 那么这个一般的命题当然不成立了, 但是可能这个命题在经过某些修改以后仍然成立, 而且有用. 那时, 反例会帮助您找到适当的修改.

于是, 教训就是: 例子是重要的. 那么, 怎样去找例子呢? 有两个完全不同的途径. 一是白手起家地去造例子. 例如, 可以定义群 G 就是一个 [正]20 面体的所有的对称的群. 另一个途径, 也是本节的主题, 是取一些已经做出来的例子, 再从它们造出新例子来. 例如, 群 $\mathbf{Z}^2$ 是由所有的整数 x 和 y"对子"(x,y) 组成的, 其中的加法是由明显的规则 $(x,y)+(x',y')=(x+x',y+y')$ 来定义的, 它就是两个群 $\mathbf{Z}$ 的 "乘积". 我们将会看到, 这个乘积的概念是很一般的, 而且可以用于许多其他的前后文条件之下. 但是让我们先来看一下甚至是更基本的找出新例子的方法.

3.1 子结构

我们已经看到, 所有复数的集合 $\mathbf{C}$, 连同其中的加法和乘法, 是域的最基本的例子之一. 它包含许多子域, 即自身也构成域的子集合 [当然要连同原来就有的运算 —— 加法和乘法]. 例如, 取所有形如 $a+b\mathrm{i}$ 的复数, 其中 a 和 b 是有理数, 它们的集合记作 $\mathbf{Q}(\mathrm{i})$. 这就既是 $\mathbf{C}$ 的子集合, 又是它的子域. 为了证明它确实是子域, 就要证明 $\mathbf{Q}(\mathrm{i})$ 对于 $\mathbf{C}$ 中的加法、乘法和取逆元也是封闭的. [而且 $\mathbf{C}$ 中的零元也在 $\mathbf{Q}(\mathrm{i})$ 中, 并且就是它的零元]. 就是说, 若 z 和 w 都是 $\mathbf{Q}(\mathrm{i})$ 的元, 则 $z+w, zw$ 也是, 同样, $-z$ 和 $1/z$(这时要求 $z\neq 0$) 也在 $\mathbf{Q}(\mathrm{i})$ 内. 加法和乘法的可交换性、结合性这些公理在 $\mathbf{Q}(\mathrm{i})$ 内也成立, 其原因很简单, 即它们在更大的集合 $\mathbf{C}$ 中是成立的.

虽然 $\mathbf{Q}(\mathrm{i})$ 包含在 $\mathbf{C}$ 中, 但是它以很重要的方式比 $\mathbf{C}$ 更有趣. 怎么会是这样呢? 人们肯定会以为, 如果把一个对象的绝大部分都拿走了, 它怎么会更有趣呢? 但是稍微进一步想一下, 就会表明这确实是可能的. 例如, 素数的集合有着一种神秘的魅力, 而不能设想, 在所有正整数的集合里会有这种魅力. 对于域, 代数的基本定理[V.13] 告诉我们每一个多项式方程在 $\mathbf{C}$ 内都有解. 这对于 $\mathbf{Q}(\mathrm{i})$ 肯定不真. 所以在 $\mathbf{Q}(\mathrm{i})$ 中, 以及在类似的域中, 可以问, 哪些多项式方程有解. 后来证明, 这是一个深刻而又重要的问题, 但在更大的域 $\mathbf{C}$ 中, 就提不出这样的问题.

一般说来, 给出了一个代数结构的例子 X, 所谓 X 的子结构就是它的一个子集合 Y, 而且具有相关的封闭性质. 例如, 群有子群, 向量空间有子空间, 环有子环 (还有理想[III.81]) 等等. 如果定义子结构 Y 的性质是一个有趣的性质, 则 Y 可能与 X 有显著的不同, 因此可能对于原来的例子库中, 又补充了一个有用的例子.

这里的讨论集中在代数, 但是在分析与几何里面, 有趣的子结构多的是. 例如, 平面 $\mathbf{R}^2$ 并不是一个很有趣的集合, 但是它有许多子集合, 至今还未充分理解, 芒

德布罗集合[III.52] 是其一例.

3.2 乘积

令 G 和 H 是两个群. 乘积群 $G\times H$ 就是以所有形如 (g,h) 的对子为元素的集合, 这里 g 在 G 中而 h 在 H 中. 这个定义告诉我们怎样从 G 的元素和 H 的元素造出 $G\times H$ 的元素来. 但是要想定义一个群, 还有更多的事情要做. 我们已经有了在 G 上和 H 上的二元运算, 需要由它们造出 $G\times H$ 上的二元运算来. 若 g_1,g_2 是 G 的元素, 而 G 中二元运算的结果, 我们已经习惯了记作 g_1g_2. 对于 H 也做类似的事情. 这时, 对于对子, 我们有明显的二元运算的定义如下:

$$(g_1,h_1)(g_2,h_2)=(g_1g_2,h_1h_2).$$

这就是说, 对于第一个坐标施以 G 中的二元运算, 而对于第二个坐标施以 H 中的二元运算.

可以用非常类似的方法来定义向量空间的乘积. 令 V 和 W 为两个向量空间, 则 $V\times W$ 的元素是对子 (v,w), 其中 v 属于 V, 而 w 属于 W. 加法和乘以标量用下面的公式来定义:

$$(v_1,w_1)+(v_2,w_2)=(v_1+w_1,v_2+w_2),$$

以及

$$\lambda(v,w)=(\lambda v,\lambda w).$$

所得的空间的维数是 V 的维数和 W 的维数之和 (这个空间更常用的记号是 $V\oplus W$, 并称为 V 和 W 的直和, 然而它是乘积的结构).

用这样简单的方法来定义乘积结构并不总是可能的. 例如, 设 $\mathbf{F}$ 和 $\mathbf{F}'$ 是两个域, 我们总会忍不住想用以下的公式来定义 "乘积域"$\mathbf{F}\times\mathbf{F}'$:

$$(x_1,y_1)+(x_2,y_2)=(x_1+x_2,y_1+y_2),$$

以及

$$(x_1,y_1)(x_2,y_2)=(x_1x_2,y_1y_2).$$

但是这样的定义并未给出一个域. 绝大多数公理都成立, 包括加法恒等元和乘法恒等元的存在 —— 它们分别是 $(0,0)$ 和 $(1,1)$—— 但是非零元素 $(1,0)$ 就没有乘法逆存在, 因为 $(1,0)$ 和 (x,y) 的乘积是 $(x,0)$, 它绝不可能是 $(1,1)$.

有时我们也能够定义更复杂的二元运算使得 $\mathbf{F}\times\mathbf{F}'$ 确实成为一个域. 例如, 取 $\mathbf{F}=\mathbf{F}'=\mathbf{R}$, 加法和上面一样, 而以不甚显然的方式定义乘法如下:

$$(x_1,y_1)(x_2,y_2)=(x_1x_2-y_1y_2,x_1y_2+x_2y_1).$$

这样, 我们会得到复数域 $\mathbf{C}$, 因为可以把对子 (x,y) 与复数 $x+yi$ 等同起来. 然而, 这样得到的并不是我们正在讨论的一般意义下的乘积域.

现在再回到群，我们前面定义的其实是 G 和 H 的直积. 但是群还有更复杂的积，可以用来造出更丰富的例子. 为了说明这一点，考虑二面体群 D_4，它是正方形的所有对称所形成的群. 这样的对称共有八个. 用 R 代表其中之一的反射，用 T 代表另一个对称，即绕原点按逆时针方向转四分之一周. 这样，每一个对称都可以写成 T^iR^j，　$i=0,1,2,3; j=0,1$(从几何上说，这个结果表示，正方形的任意对称都可以或者通过绕原点旋转 90° 的倍数得到，或者先作反射，再作旋转得到).

这就暗示，我们可以把 D_4 看作群 $\{I,T,T^2,T^3\}$(这是由 4 个旋转所成的群) 以及群 $\{I,R\}$(这是由恒等元和反射所成的群) 的某种乘积，甚至可以用记号 (T^i,R^j) 来代替 T^iR^j，然而我们必须小心. 举一个例子，现在 $(TR)(TR)$ 并不等于 $T^2R^2=T^2$，而是等于 I. 正确的乘法法则可以从以下的事实看到，这就是：$RTR=T^{-1}$(从几何上说，此式意味着，如果把一个正方形线作一个反射，再逆时针旋转 90°，最后再反射一次，其效果与顺时针旋转 90° 相同). 结果应该是

$$(T^i,R^j)(T^{i'},R^{j'})=(T^{i-i'},R^{j+j'}).$$

例如 (T,R) 与 (T^3,R) 的积应为 $T^{-2}R^2=T^2$.

以上是两个群的所谓 "半直积" 的一个简单的例子. 一般说来，给定了两个群 G 和 H，可以有好几种有趣的方式来在对子 (g,h) 的集合上定义一种二元运算，所以就有好几个潜在的可能有意思的例子.

3.3　商

我们用 $Q[x]$ 来记具有有理系数的多项式的集合，就是形如 $2x^4-3x/2-1$ 这种形式的多项式的集合. 任意两个这样的多项式，可以相加、相减和相乘，仍得同样类型的多项式. 这使得 $Q[x]$ 成为一个可换环，但不是一个域，因为若用一个多项式去除另一个多项式，结果不 (一定) 仍是多项式.

我们现在要用一个初看起来很奇怪的方法来把 $Q[x]$ 变成一个域. 方法就是，[如果是用 x^3-x-1 去除 x^5 的话]，就认为 x^3-x-1"等价于" 零多项式. 换一个方式说，就是一旦一个多项式里有 x^3 的话，就把它换成 $x+1$，并认为这样得出的新多项式等价于原来的多项式. 例如，用记号 "$\sim$" 表示 "等价于"，则有

$$x^5=x^3x^2\sim(x+1)x^2=x^3+x^2\sim x+1+x^2=x^2+x+1.$$

注意，这样一来我们可以把任意多项式换成一个次数不大于 2 的多项式，因为只要其次数更高，就可以从其中取出 x^3，把它换成 $x+1$，这样来降低次数，如我们在上面做的那样.

还要注意，当我们做了这样的代换以后，新老多项式的差将是 x^3-x-1 的 "倍式". 例如，当把 x^3x^2 换成 $(x+1)x^2$ 以后，差就是 $(x^3-x-1)x^2$. 所以，我们的做法就相当于说，两个多项式当且仅当相差 x^3-x-1 的一个 "倍式" 时，才是等价的.

我们知道, $Q[x]$ 不是一个域的原因是非常数多项式没有乘法逆. 例如, 很明显, 不能用一个多项式去乘 x^2 来得到 1. 然而, 如果用 $1+x-x^2$ 去乘它, 就会得到一个等价于 1 的多项式, 事实上, 这两个多项式的乘积是

$$x^2+x^3-x^4 \sim x^2+x+1-(x+1)x=1.$$

可以证明, 所有不等价于零的多项式 (即不是 x^3-x-1 的倍式的多项式) 都在这个广义的意义下具有乘法逆 (要求一个多项式 P 的这种广义的乘法逆, 只需用欧几里得算法[III.22] 去求两个多项式 Q 和 R 使得 $PQ+R(x^3-x-1)=1$ 就行了. 这里的右方为 1 是因为 x^3-x-1 在 $Q[x]$ 中不能分解因子, 而且 P 又不是 x^3-x-1 之倍, 所以二者的最高公因式是 1. 于是 P 的乘法逆就是 Q).

在什么意义下这意味着我们得到了一个域? 不论怎么说, x^2 与 $1+x-x^2$ 的积并不是 1, 而只是等价于 1. 商的概念就由此而来. 我们只是简单地作了如下的规定: 当两个多项式等价时, 就视这两个多项式为相等, 然后就把这样得到的数学结构记为 $Q[x]/(x^3-x-1)$. 结果是, 这样得到的结构确实是一个域, 而这个域还被证明了是很重要的, 它是包含 $Q[x]$ 和多项式 X^3-X-1 的一个根的最小的域. 这个根又是什么? 简单地就是 x[当然, 是在 $x^3-x-1\sim 0$ 的意义下]. 这里有一点微妙之处, 即我们是以两种不同的方式来看多项式的: 既把一个多项式看作 $Q[x]/(x^3-x-1)$ 的元素 (至少是在把等价多项式看成就是相等的多项式时), 又把它看作是定义于 $Q[x]/(x^3-x-1)$ 上的函数. 所以 X^3-X-1 并不是零多项式, 当 $X=2$ 时, 其值为 5, 而当 $X=x^2$ 时, 其值为 $x^6-x^2-1\sim(x+1)^2-x^2-1\sim 2x$.

您可能已经注意到, 现在对于域 $Q[x]/(x^3-x-1)$ 的讨论和 §2.2 末尾对于域 $Q(\gamma)$ 的讨论有很强的相似性. 说真的, 这不是偶然的: 它们是描述同一个域的不同方式. 然而, 把这个域看作 $Q[x]/(x^3-x-1)$ 有明显的好处, 因为它把复数的一个神秘的集合转化为关于多项式的更容易接近的问题.

把两个 "本不相等的数学对象看成相等的" 是什么意思? 关于这个问题的一个比较形式化的答案要用到等价关系和等价类的概念 (见数学的语言和语法[I.2 §2.3]). 我们说, $Q[x]/(x^3-x-1)$ 的元素其实并非多项式而是多项式的等价类. 然而, 要理解商的概念, 一个容易得多的方法是考虑一个尽人皆知的例子, 就是有理数的集合 **Q**. 如果我们试着来小心地解释什么是有理数, 我们就会这样来开始: 一个典型的有理数的形状是 a/b, 而且 $b\neq 0$. 可以定义有理数就是这种形状的表达式的集合, 而且在其中规定如下的运算法则:

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd},$$

还有

$$\frac{a}{b}\frac{c}{d}=\frac{ac}{bd}.$$

然而必须作一个非常重要的说明, 就是我们并不把任意两个这样的表达式都看成彼此相异的, 例如 1/2, 3/6 就假设是同一个有理数. 所以我们定义, 只要 $ad = bc$, 就说 a/b 和 c/d 是等价的表达式, 而等价的表达式就认为是记的同一个数. 注意, 从表达式的式子来看, 它们真的是不同的, 但是我们认为它们记的是同一个对象.

我们既已这样做了, 那么在定义函数和二元运算时就得小心了. 例如, 假如我们想用下面的看起来很自然的公式

$$\frac{a}{b} \circ \frac{c}{d} = \frac{a+c}{b+d}$$

来在 $\mathbf{Q}$ 上定义一个二元运算 "$\circ$", 这个定义就有一个非常严重的缺陷. 要问为什么, 您试着把这个公式用于分数 1/2 和 1/3, 按照这个公式会得到 2/5. 但是如果把 1/2 换成等价的分数 3/6 再用这个公式, 又会得到 4/9, 它就与 2/5 不同 [也不等价] 了. 这样一来, 虽然这个公式在形如 a/b 的表达式的集合上定义了一个完全良好的二元运算, 但是把它看作是有理数集合上的二元运算就毫无意义了.

一般说来, 必不可少的是要验明, 如果输入的是等价的对象, 那么, 输出的也必须是等价的对象. 例如, 定义域 $Q[x]/(x^3 - x - 1)$ 中的加法和乘法时, 必须验证, 如果 P 和 P' 相差 $x^3 - x - 1$ 的一个倍式, Q 和 Q' 也只相差 $x^3 - x - 1$ 的一个倍式, 则 $P + Q$ 和 $P' + Q'$ 必定也只能相差 $x^3 - x - 1$ 的一个倍式; 对于 PP' 和 QQ' 也是一样. 这是一个简单的练习.

商群是商结构的一个重要的例子. 若 G 是一个群, 而 H 是它的一个子群, 这时, 很自然地, 我们会对它做我们对于多项式所做过的事情, 而定义群的元素 g_1, g_2 当 $g_1^{-1}g_2$(很明显, 这就是 g_1, g_2 的 "差" 的概念在这个情况下的表述) 属于 H 时为等价. 容易看到, 元素 g 的等价类就是形如 gh 的元素的集合, 这里 $h \in H$ 这个等价类通常写为 gH(它叫做 H 的一个左陪集 (left coset)).

在所有左陪集的集合上有一个二元运算 $*$ 的候补者, 这就是定义 $g_1H * g_2H = g_1g_2H$, 用文字来讲, 就是在这两个左陪集里各取元素 g_1 和 g_2, 作它们的乘积 g_1g_2, 再作此乘积的左陪集 g_1g_2H. 这里又一次遇到了重要的问题: 如果从原来的左陪集里取了不同的元素, 得到的是否仍是同一个左陪集 g_1g_2H 呢? 结果是并不尽然如此. 想要它如此, 就需要对 H 加上一个附加的假设, 即 H 是一个正规子群, 这句话的意思是, 如果 h 是 H 的任意元素, 则对于群 G 的所有元素 g, ghg^{-1} 仍是 H 中的元素. ghg^{-1} 称为元素 h 的共轭元 (conjugate). 这样, 正规子群就是对于 "共轭关系为封闭" 的子群.

如果 H 是一个正规子群, 则所有左陪集的集合在上述的二元运算下成为一个群. 这个群被记作 G/H, 而被称为 G 对于 H 的商群. 可以把 G 看成 H 和 G/H 的乘积 (虽然可能是一种有点复杂的乘积), 所以, 如果懂得了 H 和 G/H, 那么对于很多的目的而言, 就可以说是懂得了 G. 所以, 没有正规子群 (除了 G 本身和恰

好由恒等元构成的子群以外, [它们是平凡的正规子群]) 的群将起特别的作用, 有点像素数在数论中的作用. 这种群称为单群 (simple group)(见*有限单群的分类*[V.7]).

为什么使用了 "商" 这个字? 商, 正常地说就是当用某个数 [例如 3] 去除 [或者说 "去分"] 另外一个数 [例如 21] 时所得到的东西. ["除法" 与 "分割" 在英语里都可以说是 "to divide", 二者本来就是相通的], 为了懂得这里面的类比, 让我们看一下怎样用 3 去除 [分]21 的. 可以想象, 这是把 21 个对象分成 3 个对象一组, 然后问一共可得几个组. 这样的分组又可以用等价关系来描述如下: 如果有两个对象被分到所得的 7 组里的同一组内, 就认为它们是等价的 [它们共同所在的组就是一个等价类]. 所以, 不等价的对象最多只有 7 个. 这样, 如果我们把同一个等价类里面的对象看作相同的, 则所谓除法就是 "按等价关系作分割", 这样得到的等价类 (共有 7 个) 的集合, 不妨就叫做 "商集合", 其中有 7 个元素, 也就是 7 个不相同的等价类.

"商" 这个概念的另一种颇不相同的用法会引导到一种很重要的数学图形环面 (torus) 的漂亮的定义, 这个图形就是一个轮胎那样的曲面 (中间有洞的那种曲面). 我们从一个平面 $\mathbf{R}^2$ 开始, 而且对于两个点 (x, y) 和 (x', y'), 当 $x-x', y-y'$ 二者均为整数时定义它们为等价的. 假设我们把等价的点看成是相同的, 而且从点 (x, y) 开始向右走, 一直走到点 $(x+1, y)$. 这一点与 (x, y) 点是 "相同" 的, 因为二者之差是 $(1,0)$, 所以好像是把整个平面卷起来成了一个竖直的周长为 1 的圆柱面, 而刚才的行走就好比是环绕了这个圆柱面一次. 如果对 y 轴也进行一次刚才的论证, 注意到点 (x, y) 和点 $(x, y+1)$ 总是 "同一点", 我们就会看到, 这个柱面又被 "折成了圈", 所以, 如果 "往上走" 了一段距离为 1, 就又回到了出发地. 但是这就是一个环面: 一个自己折成圈的柱面 (然而, 这不是定义环面的唯一的方法, 例如还可以把它定义为两个圆周的乘积).

现代几何的许多对象都是用商来定义的. 时常有这样的情况: 一个对象极大, 但同时等价关系又很宽松, 就是说一个对象很容易就与另一个对象等价了. 在这个情况下, "真正相异的" 对象的数目可能很小. 这当然只是一个很粗疏的说法, 因为真正有意思的并不是相异对象的数目, 而是这些对象的集合之复杂性. 比较好的说法是: 时常是从一个大得令人绝望而又极为复杂的对象出发, 但是 "把绝大部分的乱七八糟都分出来除掉了", 结果得到的商结构却足够简单而能够处理, 而仍旧传递重要的信息. *基本群* [IV.6 §2]、*拓扑空间的同调群与上同调群* [IV.6 §4]都是好例子, 而*模空间*[IV.8] 甚至是一个更好的例子.

许多人觉得商这个概念多少比较难懂, 但它在整个数学中有很大的重要性, 这就是为什么要在这里比较详细地加以讨论的原因.

4. 代数结构之间的函数

一个几乎无例外的规则是, 对于数学结构是从来不孤立地进行研究的, 我们在

研究这些结构的同时, 还要研究定义在这些结构上的函数. 在本节里面, 我们要考虑有哪些函数值得考虑以及为什么 (关于函数的一般讨论, 请参看**数学的语言和语法**[I.2 §2.2]).

4.1 同态, 同构和自同构

如果 X 和 Y 是某一个特定的数学结构的两个例子, 例如同是群、域或向量空间, 那么如同我们在 §2.1 中讨论对称性时提到过的那样, 有一类从 X 到 Y 的函数特别有意义, 具体说就是 "保持结构" 的那些函数. 粗略地说, 一个函数 $f: X \to Y$ 保持 X 的结构, 就是说, 如果 X 中的元素之间存在着一个用这个结构来表示的关系, 则这些元素的像之间也存在着用 Y 的结构来表示的同样的关系. 举例来说, 设 X 和 Y 是群, 而 a, b, c 是 X 的元素, 而且 $ab = c$, 那么如果 f 保持 X 的结构, 则在 Y 中必有 $f(a)f(b) = f(c)$(这里采用通常的做法, 即用乘法的记号来表示使得 X 和 Y 是群的那个二元运算). 与此类似, 若 X 和 Y 是域, 而我们用通常表示加法和乘法的标准记号来表示其中的二元运算, 则只有适合以下关系的函数 $f: X \to Y$ 才是有意义的: 当 $a + b = c$ 时, $f(a) + f(b) = f(c)$; $ab = c$ 时 $f(a)f(b) = f(c)$. 对于向量空间, 有意义的函数就是保持线性组合的函数: 若 V, W 是向量空间, 则 $f(av + bw) = af(v) + bf(w)$.

一个保持结构的函数就称为一个同态 (homomorphism), 然而, 特定的数学结构的同态常有专门的名字, 例如向量空间的同态就称为线性映射.

如果我们有好运气, 同态就可能有一些有用的性质. 为了明白为什么具有这些进一步的性质是值得的, 请看下面的例子. 设 X 和 Y 是群, 而 $f: X \to Y$ 把 X 的任意元素都映为 Y 的恒等元 e. 按照上面的定义, 这个 f 就是保持结构的函数, 因为只要 $ab = c$, 则必有 $f(a)f(b) = ee = e = f(c)$. 然而, 这时我们说 f 使得原有的结构都坍塌了. 更准确一些. 可以把这里的思想说得更确切一点, 虽然当 $ab = c$ 时, $f(a)f(b) = f(c)$, 其逆则不成立. 完全有可能 $f(a)f(b) = f(c)$ 而 ab 并不等于 c, 实际上, 上面的例子正是这个情况.

两个结构 X 和 Y 间的同构就是这样一个同态 $f: X \to Y$, 其逆 $g: Y \to X$ 也是一个同态. 对于绝大多数代数结构 [例如群], 可以证明, 若 f 有逆 g, 则 g 自动地也是同态, 在这种情况下, 我们可以说同构就是同时也是**双射**[I.2 §2.2] 的同态. 就是说, f 是 X 和 Y 之间的保持结构的一对一的对应[①].

---

① 我们来看对于群是怎样证明 g 自动地也是同态的. 设 X 和 Y 是群, 而 $f: X \to Y$ 是一个同态, 而且有逆 $g: Y \to X, u, v, w$, 则设为 Y 的元素, 而且 $uv = w$, 需要证明 $g(u)g(v) = g(w)$. 为此, 令 $a = g(u), b = g(v)$ 以及 $d = g(w)$. 因为 f 和 g 互为反函数, 所以 $f(a) = u, f(b) = v$ 以及 $f(d) = w$. 现在令 $c = ab$. 于是 $w = uv = f(a)f(b) = f(c)$, 因为 f 是一个同态. 但是这样就有 $f(c) = f(d)$, 这就意味着 $c = d$(只要用 g 作用于 $f(c)$ 和 $f(d)$ 就可以看到这一点). 因此 $ab = d$, 这就告诉我们 $g(u)g(n) = g(w)$. 这就是需要证明的事情.

若 X 和 Y 是域, 这些考虑就不那么有趣了, 证明每一个同态 $f: X \to Y$ 是 X 及其像 $f(X)$(就是函数所取的值的集合) 自动地成为同构, 只是一个简单的练习. 所以结构不可能只是坍塌而不会失去 (这个证明依赖于 Y 中的零没有乘法逆这一事实).

一般地说, 两个代数结构 X 和 Y 间若有同构的函数关系, 就说 X 同构于 Y(同构 (isomorphism) 一词的语源是希腊字 isos-(意为 "相同") 和 -morph(意味 "形状")). [其实同态 (homomorphism) 一词也来自 homo-(意思也是 "相同") 和 morph]. 粗略地说, "同构" 这个词的意思就是 "在所有本质的方面都相同", 而哪些方面算是本质的? 那就是指代数结构. 什么是绝对非本质的呢? 那就是具有这种结构的对象自身的本性. 例如, 一个群可能是由复数组成的, 而另一个群可能来自整数 mod 一个素数 p, 第三个群则可能是几何图形的旋转所成的, 而这三个群却可能是同构的. 两个数学结构可能有非常不同的组成成分, 然而却在更深的意义下是 "相同的", 这个思想是数学的最重要的思想之一.

代数结构 X 到其自身的同构称为自同构. 既然毫不奇怪, X 必与其自身同构, 所以就要问, 自同构的要点究竟何在? 答案是, 自同构就是我们在讨论群的时候所暗指的代数对称性. X 的自同构就是由 X 到其自身的保持结构的函数 (这种结构现在以 $ab = c$ 这类命题的形式出现). 两个自同构的复合很清楚是第三个自同构, 结果是结构 X 的自同构也构成一个群. 虽然个别的自同构不一定很有意思, 自同构的群却是大有意思, 它时常蕴含了我们关于一个结构真正想知道的事, 而这个结构时常太复杂, 不能直接分析.

在 X 为一个域的情况, 可以看到这一点的一个蔚为壮观的例子. 为了说明这一点, 现以 $\mathbf{Q}(\sqrt{2})$ 为例. 若 $f: \mathbf{Q}(\sqrt{2}) \to \mathbf{Q}(\sqrt{2})$ 是一个自同构, 则 $f(1) = 1$(这可以容易地从 1 是 $\mathbf{Q}(\sqrt{2})$ 中仅有的乘法恒等元看出来). 由此可得 $f(2) = f(1+1) = f(1) + f(1) = 1 + 1 = 2$. 继续下去就有 $f(n) = n$, n 为任意正整数. 然后有 $f(n) + f(-n) = f(n + (-n)) = f(0) = 0$, 所以 $f(-n) = -f(n) = -n$, 最后还有 $f(p/q) = f(p)/f(q) = p/q$, 这里 p, q 是 1 任意整数而且 $q \neq 0$. 所以 f 把每一个有理数都变成其自身. 那么它又把 $\sqrt{2}$ 变成什么呢? 事实上, $f(\sqrt{2})f(\sqrt{2}) = f(\sqrt{2} \cdot \sqrt{2}) = f(2) = 2$, 但这就蕴含 $f(\sqrt{2})$ 是 $\sqrt{2}$ 或 $-\sqrt{2}$. 结果是两种选择都是可以的, 有一个自同构是 "平凡的", 即 $f(a + b\sqrt{2}) = a + b\sqrt{2}$, 另外一个则比较有趣, $f(a + b\sqrt{2}) = a - b\sqrt{2}$. 看到了这一点就证明了两个平方根并没有代数上的区别. 在这个意义上 $\mathbf{Q}(\sqrt{2})$ 并不知道哪一个平方根为正, 哪一个为负. 这两个自同构形成一个群, 这个群既同构于 ± 1 在乘法下所成的群, 也同构于整数 mod2 的群, 还同构于非等边的等腰三角形的对称所成的群 ······ 这样的清单还可以无限地写下去.

与某一个域扩张相关的自同构群称为伽罗瓦群, 对于*五次方程的不可解性*[V.21]以及*代数数论*[IV.1] 的很大一部分, 它都是生命攸关的.

和代数结构的同态 ϕ 相关的一个重要概念是它的核的概念. 核定义为 X 中所有使得 $\phi(x)$ 为 Y 中的恒等元的那些 x 的集合 (当 X 和 Y 涉及加法和乘法两个二元运算时, 这里说的恒等元仅指加法恒等元). 同态的核时常是 X 的具有有趣性质的子结构. 例如说, 如果 G 和 K 是群, 则由 G 到 K 的同态的核是 G 的一个正规子群; 反过来, 若 H 是 G 的在正规子群, 则把 G 的一个元素 g 映为左陪集 gH 的商映射是由 G 到商群 G/H 的一个同态而以 H 为核. 类似地, 环同态的核必是一个理想[III.81], 而环 R 的每一个理想 I, 又都是由 R 到 R/I 的 "商映射" 的核 (这个商结构将在条目环, 理想与模[III.81] 中更详细地讨论).

4.2　线性映射和矩阵

向量空间的同态具有区别于其他函数的几何性质：它们把直线映为直线. 由于这个原因, 它们被称为线性映射, 这一点已经在前一小节提到过. 从比较代数的观点来看, 线性映射所保持的代数结构就是线性组合. 若 f 是从一个向量空间 V 到另一个向量空间 W 的函数, 若对每一对元素 $u, v \in V$ 和每一对标量 a, b 都有 $f(au+bv) = af(u) + bf(v)$, 则 f 是一个线性映射. 由此可以得到一个比较更一般的断言：对于线性映射 f, $f(a_1v_1 + a_2v_2 + \cdots + a_nv_n)$ 总是等于 $a_1f(v_1) + a_2f(v_2) + \cdots + a_nf(v_n)$.

设我们想定义一个由 V 到 W 的线性映射, 需要提供多少信息才行呢？为了看清这里需要的是什么样的答案, 我们来看一个比较容易的问题：为了确定一点在空间的位置, 需要多少信息？答案是：只要我们已经定下了一个合理的坐标系, 三个数就够了. 如果这个点离地球表面不太远, 举例来说, 我们可以就用此点的经度、纬度和它在海平面上方的高度为这三个数. 一个由 V 到 W 的线性映射是不是也可以仅用很少几个数就能确定呢？

答案是：可以. 至少当 V 和 W 是有限维空间时可以. 设 V 有一组基底 $v_1, \cdots, v_n$, W 也有一组基底 $w_1, \cdots, w_m$, 而 $f: V \to W$ 是我们想要确定的线性映射. 因为 V 中的每一个向量都可以写成 $a_1v_1 + \cdots + a_nv_n$, 而 $f(a_1v_1 + \cdots + a_nv_n)$ 又总等于 $a_1f(v_1) + \cdots + a_nf(v_n)$, 所以, 只要我们能够确定 $f(v_1), \cdots, f(v_n)$ 是什么, 就能完全确定 f 了. 但是, 每一个向量 $f(v_j)$ 又是基底向量 $w_1, \cdots, w_m$ 的线性组合, 所以它就可以写成

$$f(v_j) = a_{1j}w_1 + \cdots + a_{mj}w_m$$

的形式. 这样, 为了确定每一个 $f(v_j)$, 就需要 m 个数, 即标量 $a_{1j}, \cdots, a_{mj}$. 因为一共有 n 个不同的向量 v_j, 所以一个需要 mn 个数, 即标量 a_{ij}. 这里 i 从 1 变到 m, 而 j 从 1 变到 n. 我们把这 mn 个标量排成

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}.$$

这样一个阵, 称为一个矩阵. 重要的是要注意, 如果取 V 和 W 的不同的基底, 就会得到不同的矩阵. 所以我们称此矩阵为 f 相对于这一对基底 (V 和 W 各一组基底) 的矩阵.

现在设 f 是一个由 V 到 W 的线性映射, 而 g 是一个由 U 到 V 的线性映射, 则 fg 代表由 U 到 W 的如下的线性映射：先作 g, 再作 f. 如果 f 和 g 相对于 U, V 和 W 的各一组基底的矩阵, 分别是 A 和 B, 那么 fg 的矩阵是什么？为了把它算出来, 取 U 的基底 u_k 并且让 g 作用于它, 从而得出 V 的基底向量的线性组合 $b_{1k}v_1 + \cdots + b_{nk}v_n$. 再把 f 作用于其上, 又得到 W 的基底向量 $w_1, \cdots, w_m$ 的"线性组合的线性组合"的非常复杂的表达式.

追随这样的想法, 我们可以计算出 fg 的矩阵 P 的第 i[横] 行第 j[竖] 列的元素是 $a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{in}b_{nj}$, 这个矩阵称为矩阵 A 和矩阵 B 的乘积. 如果您过去没有见过这个定义, 就会觉得它很难掌握, 但是需要记住的主要之点只是：有一个办法可以从 f 和 g 的矩阵 A 和矩阵 B 算出 fg 的矩阵来, 而这个矩阵就记作 AB. 矩阵的这种乘法是结合的, 但一般是不可交换的, 就是说, $A(BC)$ 总是等于 $(AB)C$; 但是 AB 不一定等于 BA. 结合性可以从下面的事实得出, 即矩阵下面的线性映射的复合运算是结合的：若 A, B 和 C 分别是 f, g 和 h 的矩阵, 则 $A(BC)$ 是以下的线性映射"先作 h 后面跟着 g, 然后作 f"的矩阵, 而 $(AB)C$ 则是线性映射"先作 h 然后作 g 后面跟着 f"的矩阵, 二者是同样的线性映射.

我们现在限于只看从一个向量空间 V 到其自身的自同构. 它们就是可逆的线性映射 $f : V \to V$. 就是说, 对于它们存在一个线性映射 $g : V \to V$ 使得对于 V 中的每一个向量 v 都有 $fg(v) = gf(v) = v$. 可以把它们看作向量空间 V 的一种"对称", 这样, 它们就在复合之下构成一个群. 如果 V 是 n 维的, 而标量来自域 $\mathcal{F}$, 这个群就叫做 $\mathrm{GL}_n(\mathcal{F})$. 这里的字母 G 代表"general"(一般), L 代表"linear"(线性)[而这个群就称为 n 阶一般线性群]. 数学中一些最重要、最困难的问题时常来自试图去理解某一个有趣的域 $\mathcal{F}$ 上的一般线性群 (及其相关的群) 的结构 (见**表示理论**[IV.9§§5,6]).

尽管矩阵是很有用的, 许多有趣的线性映射却是无限维向量空间之间的映射. 所以我们为那些熟悉初等的微积分的读者 (本文后面有一小节对微积分作简短的讨论) 讲两个例子作为本节的结束. 第一个例子, 设 V 是所有的由 $\mathbf{R}$ 到 $\mathbf{R}$ 的可以微分的函数的集合, 又令 W 为所有的由 $\mathbf{R}$ 到 $\mathbf{R}$ 的函数的集合. 它们都可以简单的方

式做成向量空间：若 f 和 g 是函数，它们的和就是由公式 $h(x)=f(x)+g(x)$ 所定义的函数 h，而若 a 是一个实数，则 af 是由公式 $k(x)=af(x)$ 所定义的函数 k(这样，举例来说，多项式 x^2+3x+1 就是函数 x^2, x 和常值函数 1 的一个线性组合). 这样，微分就是一个 (由 V 到 W 的) 线性映射，因为导数 $(af+bg)'$ 就是 $af'+bg'$. 如果用 $\mathrm{D}f$ 来表示导数，这一点就会更清楚，因为现在有 $\mathrm{D}(af+bg)=a\mathrm{D}f+b\mathrm{D}g$.

第二个例子要用到积分. 令 V 为另一个函数的向量空间，而 u 是两个变量的函数 (所用到的函数还要有一些性质，定义才有意义，但是我们略去技巧问题). 这时可以用公式

$$(Tf)(x)=\int u(x,y)f(y)\mathrm{d}y$$

来定义空间 V 上的一个线性映射 T. 像这样的定义可能难以接受，因为这样的定义包含了三个层次的复杂性. 在最底下的一层，有两个实数，记作 x 与 y. 中间的一层则有以下函数如 f, u 还有 Tf. 在顶层还有另一个函数 T，但是这一次它要加以变换的 “对象” 本身也是函数：它要把 f 这样的函数变成另一个函数 Tf. 这是一个例子，即要把一个函数看成一个单个的、原始的 “东西”，而不是 [把一个变量变为另一个变量的] 过程 (见**数学的语言和语法**[I.2 §2.2] 中关于函数的讨论). 另一个有助于弄清定义的说明是，二元函数 $u(x,y)$ 的作用与矩阵 (a_{ij})(它也可以看成是两个整数值变量 i,j 的函数) 的作用有着深刻的类比. 像 u 这样的函数有时也叫做核 (这不应与同态的核相混淆). 关于无限维空间之间的线性映射，更多地可以参看**算子代数**[IV.15] 和**线性算子**[III.50]).

4.3 本征值和本征向量①

令 V 为一个向量空间，而 $S: V\to V$ 为由 V 到其自身的线性映射. 所谓 V 的本征向量就是 V 的一非零向量 v 使得 Sv 与 v 成比例，即有一个标量 λ 使得 $Sv=\lambda v$. 这个 λ 称为相应于 v 的本征值. 这个简单的定义极为重要，很难想到有哪一个数学领域，本征向量和本征值不在其中起重要作用. 但是为什么 Sv 与 v 成比例会这么有趣？大体上说，这是由于在许多情况下，线性映射的本征向量与本征值，包含了我们所需的关于这个线性映射的信息，而且是以很方便的形式包含它们. 另一个回答则是线性映射出现在许多不同前后文的环境下，而在这些情况下出现的问题又时常是关于本征向量和本征值的问题. 下面是两个例子.

第一个例子，设想有了一个由向量空间 V 到其自身的线性映射 T，我们想了解，如果逐次反复使用 T 会发生什么. 处理方法之一是：取 V 的一组基底，并且算出 T 在此基底下的矩阵 A，然后我们就用矩阵乘法去计算 A 的各次幂. 麻烦在于

① 本征这个字头原来来自德文 eigen，意思是固有的、特有的、内在的，等等. 因此在许多中文文献中，常译为 “固有”“特征” 等等. 现在按照《数学百科全书》(科学出版社) 的译法，译为 “本征”.—— 中译本注

这里的计算会是乱成一团, 不能提供什么信息. 这个方法对于此线性映射没有给出真正的洞察.

然而, 时常可以取一个特殊的由本征向量组成的基底, 这时, 了解 T 的各次幂就很容易了. 事实上, 令基底向量为 $v_1, v_2, \cdots, v_n$, 而每一个 v_i 又是相应于本征值 λ_i 的本征向量: 就是设对于每一个 i 都有 $Tv_i = \lambda_i v_i$. 如果 w 是 V 中的任意向量, 则有恰好一种方法把 w 写成 $a_1v_1 + \cdots + a_nv_n$, 于是

$$Tw = \lambda_1 a_1 v_1 + \cdots + \lambda_n a_n v_n.$$

粗略地说, 这说明 T 把 w 的 v_i 方向的各个成分分别按因子 λ_i 拉伸. 现在就容易说明, 如果我们不止对 w 使用 T 一次, 而是使用 m 次, 会出现什么情况了. 结果将是

$$T^m w = \lambda_1^m a_1 v_1 + \cdots + \lambda_n^m a_n v_n.$$

换句话说, 现在对 w 的 v_i 方向的成分上我们做了因子为 λ_i^m 的拉伸, 这就是全部问题所在.

为什么我们会有兴趣一而再地做同一个线性映射? 有许多理由要这样做 —— 一个现代的有说服力的理由是: 谷歌在把网址排成有用的次序时, 就是用的这种计算, 详见*算法设计的数学*[VII.5].

第二个例子是关于*指数函数*[III.25]e^x 的有趣的性质的, 这个性质就是: 指数函数的导数是同一个函数. 换句话说, 若 $f(x) = \mathrm{e}^x$, 则 $f'(x) = f(x)$. 我们前面已经看到, 微分运算可以看成是一个线性映射, 而若 $f'(x) = f(x)$, 则此映射使得函数 f 不变, 这说明此函数是一个本征向量, 其本征值为 1. 比较一般地, 若令 $g(x) = \mathrm{e}^{\lambda x}$, 则 $g'(x) = \lambda\mathrm{e}^{\lambda x} = \lambda g(x)$, 所以 g 也是微分映射的本征向量, 但这一次相应的本征值是 λ. 许多线性微分方程都可以看成是要求由微分定义的线性映射的本征向量 (微分和微分方程将在下一节讨论).

5. 数学分析的基本概念

由于微积分的发明和下面概念的出现, 可以通过越来越好的近似来间接刻画一个数学对象的概念的出现, 数学在其精巧性上得到了一个巨大的飞跃. 这些思想成了数学的一个广阔领域, 即所谓分析的基础, 而本节的目的就是给那些尚不熟悉于此的读者一点帮助. 然而, 对它给出完备的准确的介绍是不可能的, 若对微积分事先没有最低限度的了解, 这里所写的内容也是很难懂得的.

5.1 极限

在关于实数的一节 (§1.2) 里, 我们对于 2 的平方根做过简短的讨论. 我们是怎样知道 2 有平方根的? 下面是一种回答: 是通过计算它的十进小数展开式. 如果想要

回答得更准确一点, 就可以这样说, 实数 $1, 1.4, 1.41, 1.414, 1.4142, 1.41421, \cdots$(它们都是有尽小数, 所以是有理数) 会趋近另一个实数 $x = 1.4142135\cdots$. 我们不能真正地适当写出 x 来, 因为它的十进小数展开式是无尽的, 但是我们至少可以说明它的各位数值是怎样确定的, 例如, 小数点后的第三位是 4, 因为 1.414 是其平方仍然小于 2 的 0.001 的最大的倍数. 由此可知, 原来那一串数的平方 $1, 1.96, 1.9881, 1.999396, 1.99996164, 1.9999899241, \cdots$ 趋向 2, 这就是我们何以有权说 $x^2 = 2$ 的理由.

假设要求我们决定画在一张纸上的一段曲线的长度, 而且给了一支直尺来帮忙. 我们就遇到了一个问题: 直尺是直的而曲线是弯的. 对付这个问题的一种方法如下: 首先, 沿曲线画几个点 $P_0, P_1, P_2, \cdots, P_n$, 一端是 P_0 而另一端是 P_n. 然后, 度量从 P_0 到 P_1 的距离, 从 P_1 到 P_2 的直线距离, 如此直到 P_n. 最后, 把这些直线距离加起来. 结果并不恰好就是正确的答案, 然而, 如果点取得足够多, 其分布又合理地平均, 而这曲线又不太弯来弯去, 我们的程序对于 "近似长度" 就会给出一个很好的概念. 此外, 这个程序还会给我们一个方法来定义 "准确长度" 的确切意义: 假如我们取越来越多的点, 又发现上述意义下的近似长度会趋近某一个数 l. 这时, 我们就会说曲线的长度是 l.

这两个例子里面都有一个数, 我们是通过逐步逼近来达到的. 在这两个例子里都用了 "逼近" 一词, 但是它的意义有点含糊, 把它弄准确是很重要的. 令 $a_1, a_2, a_3, \cdots$ 为一串实数. 说这些实数趋近于一个特定的实数 l 是什么意思?

下面两个例子很值得熟记在心. 第一个是序列 $1/2, 2/3, 3/4, 4/5, \cdots$. 在某种意义下也可以说这个序列趋近于 2[①], 因为每一项都比前一项离 1 更近, 但是很清楚, 我们所谓趋近于 1 并不是这个意思. 真正是关键的并不在于各项离 1 越来越近, 而在于我们能够任意地接近, 只有一个数值是这个序列能够在这个较强意义下能够趋近的数值, 它就是显然的 "极限"1.

第二个例子用一种不同的方式说明这一点. 这就是序列 $1, 0, 1/2, 0, 1/3, 0, 1/4, 0, \cdots$. 在这里我们愿意说这些数趋近于 0, 虽然并非每一项都比前一项更接近 0. 然而, 有一点是真的, 那就是这个序列最终会离 0 要多近就有多近, 而且以后一直至少那么近.

"要多近就有多近, 而且以后一直至少那么近" 这个句子就是极限的数学概念的定义: 数的序列 $a_1, a_2, a_3, \cdots$ 的极限是 l, 如果这个序列最终会离 l 要多近就有多近, 而且以后一直至少那么近. 然而为了符合数学对于精确性所要求的标准, 我们需要把诸如 "最终" 之类的日常语言翻译成数学语言, 为此就要用到量词[I.2 §3.2].

设 δ 为一正数 (通常设想它很小), 如果 a_n 与 l 的距离 $|a_n - l|$ 小于 δ, 就说 a_n δ- 逼近于 l. 说这个序列最终 δ- 逼近于 l 而且以后一直至少那么近, 这又是什

① 原书误为 2. —— 中译本注

么意思呢？这就是说"从某一点往后，所有的 a_n 都 δ- 逼近于 l". 什么由叫做"从某一点往后"呢？就是说有一个数 N(这个数就是那个"点") 具有以下性质：从 N 往后 —— 就是对于所有大于或等于 N 的数 n—a_n 都会 δ- 逼近于 l，用符号来写，就是

$$\exists N, \forall n \geqslant N, a_n \text{ 都 } \delta\text{- 逼近 } l.$$

余下的还要弄清楚"要多近就有多近"是什么意思. 这就是说对于任何一个您想要指定的 δ，这个句子都真 [成立]. 用符号来写就是

$$\forall \delta, \exists N, \forall n \geqslant N, a_n \delta\text{- 逼近于 } l.$$

最后，我们要停止使用不标准的短语"δ- 逼近于 l"，于是得到

$$\forall \delta, \exists N, n \geqslant N, |a_n - l| < \delta.$$

这个句子不那么容易懂. 不幸的是 (按照 [I.2 §4] 的讨论来看，有意思的也就在此) 使用下面那种不那么符号化的语言，也没有能使事情容易多少：不论如何取正数 δ，都有一个数 N，使得对于较大的数 n，a_n 与 l 的距离小于 δ.

极限的概念用于比数广泛得多的范围. 如果有一族数学对象，又能够说得出任意两个这种对象的距离，就可以说，这种对象的序列有极限的问题. 两个对象，如果其距离小于 δ(不说其差小于 δ)，就说它们是 δ- 逼近的 (距离的概念将在*度量空间*[III.56] 里进一步讨论). 例如空间里的点的序列可以有极限，函数序列也可以有极限 (在第二种情况下，如何定义距离不那么明显，但是有多种很自然的途径来做这件事). 一个进一步的例子来自分形理论 (见*动力学*[IV.14])，在那里出现的很复杂的图形最好是定义为较简单的图形的极限.

"序列 $a_1, a_2, \cdots$ 的极限是 l"这句话还有两种说法：一是"a_n 收敛于 l"，一是"a_n 趋向 l"，有时还会加上"当 n 趋向无穷时"如何如何. 任何一个有极限的序列都称为收敛的，a_n 收敛于 l 时常记作 $a_n \to l$.

5.2 连续性

假设您想要知道 π^2 的近似值，也许最简单的是在计算器上按下按钮 π，显示出 3.1415927，然后再按 x^2 按钮，又得出 9.8696044. 当然您知道计算器并没有对 π 做出准确值的平方，相反，它只是做了 3.1415927 的平方 (如果您的计算器是一个好计算器，它会秘密地使用 π 的多几位小数值，而又不显示这件事，但是它没有使用无限多位小数). 为什么计算器做了一个错误的数的平方而不会出什么问题呢？

第一个答案是所需要的只是 π^2 的近似值. 但这还不是一个完全的解释，我们怎么能知道，如果 x 是 π 的一个好的近似，那么 x^2 也会是 π^2 的一个好近似值呢？下面给出人们会怎样说明这一点的. 如果 x 是 π 的一个好的近似，就可以写出 $x = \pi + \delta$，而 δ 是一个很小的数 (可能是负的)，于是 $x^2 = \pi^2 + 2\pi\delta + \delta^2$. 因为 δ 很小，所以 $2\delta\pi + \delta^2$ 也很小，于是 x^2 也就是 π^2 的好近似值.

是什么使得上面的推理有效? 那就是把 x 变为其平方的函数是连续的. 粗略地讲, 这意味着如果两个数很接近, 则它们的平方也很接近.

为了把连续性说得更精确一点, 我们现在回到 π^2 的近似计算, 而且设想我们希望把它做得精确得多 —— 例如使得小数点后的前 100 位数都是正确的. 这时计算器不会有大的用处, 但是我们可以找到 π 的十进小数展开式的各位数值 (可以在因特网上找到这样的网址, 它可以告诉您至少 5000 万位), 用它来作为新的 x, 这个 x 是 π 的一个好得多的近似值, 找一台电脑来做必要的很长的乘法, 就能得出新的 x^2.

如果想要 x^2 是 π^2 的误差在 10^{-100} 之内的近似值, x 需要接近 π 到何种程度? 为了回答这个问题, 我们回到前面的推理. 再令 $x = \pi + \delta$, 于是 $x^2 - \pi^2 = 2\delta\pi + \delta^2$, 做简单计算就知道, 如果 δ 的模小于 10^{-101}, 则这个差的模就会小于 10^{-100}. 所以, 只要取 π 的前 101 位小数正确就行了.

比较一般地说, 不论我们希望对 π^2 的估计达到多么精确, 只要准备使得 x 是 π 的一个充分好的近似, 就总能够达到这个精确度. 用数学的语言来说就是: 函数 $f(x) = x^2$ 在 π 点是连续的.

让我们更多地用符号来说明这一点. "在精确度 ε 之内, $x^2 = \pi^2$" 这个命题的意思是 $|x^2 - \pi^2| < \varepsilon$. 所谓使 $x^2 = \pi^2$"达到任意的精确度", 就是要求上述不等式对于任意的 ε 都成立. 所以, 我们应该先说 $\forall\varepsilon > 0$. 现在再来看 "只要我们准备使得 x 是 π 的一个充分好的近似" 这句话, 这里面的思想就是有一个 $\delta > 0$, 使得只要 x 离 π 之差在 δ 之内, 则可以保证近似的精确度在 ε 之内. 这就是说, 存在一个 $\delta > 0$, 使得若 $|x - \pi| < \delta$, 就可以保证 $|x^2 - \pi^2| < \varepsilon$. 把这一切都放到一起, 就得到下面的符号语句:

$$\forall\varepsilon > 0, \exists\delta > 0, (|x - \pi| < \delta \Rightarrow |x^2 - \pi^2| < \varepsilon).$$

用通常的语言来说就是: "给定任意正数 ε, 必有一个正数 δ, 使得若 $|x - \pi|$ 小于 δ, 则有 $|x^2 - \pi^2| < \varepsilon$. " 前面我们已经找到了一个 δ, 使得当 ε 为 10^{-100} 时, 可以做到这一点, 这个 δ 就是 10^{-101}.

我们已证明了函数 $f(x) = x^2$ 在点 $x = \pi$ 处连续. 现在我们把这个概念加以推广: 令 f 为任意函数, 而 a 为任意实数. 我们说 f 在 a 处连续, 如果

$$\forall\varepsilon > 0, \exists\delta > 0, (|x - a| < \delta \Rightarrow |f(x) - f(a)| < \varepsilon).$$

这句话就是, 不论您希望 $f(x)$ 是 $f(a)$ 的何等精确的估计, 只要准备让 x 是 a 的一个充分好的近似, 这种精确度都是可以达到的. 说函数 f 是连续的, 就是说它在每一点 a 处都连续. 粗略地说, 就是 f 没有 "突然的跳跃"(它也排除了某些类型的迅速的振荡, 因为那也会使精确的估计很难).

和极限的情况一样, 连续性的思想也可用于更一般的场合下, 而且理由也相同. 令 f 是由一个集合 X 到另一个集合 Y 的函数, 而且设有两个距离概念, 其中一

个适用于 X 的元素, 另一个适用于 Y 中的元素. 用 $d(x,a)$ 表示 x 和 a 的距离, $d(f(x),f(a))$ 表示 $f(x)$ 和 $f(a)$ 的距离, 我们说 f 在 a 处连续, 如果

$$\forall\varepsilon > 0, \exists\delta > 0, (d(x,a) < \delta \Rightarrow d(f(x), f(a) < \varepsilon)).$$

而如果 f 在 X 的每一点 a 都连续, 就说 f 在 X 上连续.

连续函数也和同态一样, 可以看成是保持了某种结构的. 可以证明, 一个函数在 a 点连续当且仅当 $a_n \to a$ 时必有 $f(a_n) \to f(a)$. 这就是说, 连续函数就是那种保持由收敛序列及其极限所提供的结构的函数.

5.3 微分

函数 f 在 a 点的导数, 通常是作为量度 $f(x)$ 在 x 通过 a 点处的变化率的一个数来提出的. 本节的目的是要推介一种稍有不同的看待它的方法, 这个方法更为一般, 而且打开了通向很大一部分现代数学的门户. 这个思想就是微分作为一种线性近似.

直观地, $f'(a) = m$ 就是说, 如果用一个非常强有力的显微镜在包含点 $(a, f(a))$ 的一个微小的区域里去观看 f 的图像, 则我们看到的, 几乎恰好就只是一条梯度 (即斜率) 为 m 的直线. 换句话说, 在点 a 的充分小的邻域里, 函数 f 近似地为线性函数. 我们甚至可以把这个作为 f 的近似的线性函数 g 写出来:

$$g(x) = f(a) + m(x - a),$$

这是过点 $(a, f(a))$ 而梯度为 m 的直线的方程. 另一个比较清楚的写法是

$$g(a + h) = f(a) + mh.$$

说 g 在点 a 的一个小邻域里逼近 f, 就是说当 h 很小时, $f(a + h)$ 近似地等于 $f(a) + mh$.

在这里必须小心一点: 说到头来, 只要 f 不发生突然的跳跃, 则当 h 很小时, $f(a + h)$ 总是很接近于 $f(a)$, 而 mh 总是很小, 从而 $f(a + h)$ 总是近似地等于 $f(a) + mh$. 这样的思路似乎不论 m 是什么数都是可以的, 然而我们需要的是, 当 $m = f'(a)$ 时, 会发生什么特别的情况. 把 $m = f'(a)$ 这个特殊的值单独提出来, 并不仅仅在于 $f(a+h)$ 接近于 $f(a)+mh$, 而且在于它能够使二者接近到这样的地步, 即差 $\varepsilon(h) = f(a+h) - f(a) - mh$ 比较 h 更小. 就是说当 $h \to 0$ 时, $\varepsilon(h)/h \to 0$(这是一个比 §5.1 中所讨论的极限概念 [更强] 的极限概念. 它是说, 可以把 $\varepsilon(h)/h$ 变得如所需要的那么小, 只要取 h 足够小就可以了).

这些概念能够推广的理由是: 线性映射的概念并不简单地只是一个由 $\mathbf{R}$ 到 $\mathbf{R}$ 的形如 $g(x) = mx + c$ 的函数, 它还要广泛得多. 许多在数学中自然出现 —— 其实

在科学、工程、经济和许多其他领域里也自然出现的函数都是多元函数, 所以可以看作是定义在一个维数大于 1 的向量空间里的函数. 只要采用了这种观点, 立刻就会问, 它们能否在一点的一个小邻域中, 用线性映射去逼近. 如果能, 那就非常有用了, 一个一般的函数, 性态可以极为复杂, 但是如果能用线性函数去逼近它, 至少在 n 维空间的一个小邻域里, 它的性态就容易理解多了. 这时, 可以用线性代数和矩阵的工具, 这些工具会导出切实可行的计算, 至少在借助于计算机时, 这些计算是切实可行的.

举例来说, 想象一个气象学家, 他在观测地球上空某个 3 维区域时, 关心风在不同地点的方向和速度的变化. 风的性态是非常复杂的, 甚至是混沌的, 但是为了得到对它的某种程度的掌握, 可以这样来描述它. 对此区域的每一点 (x,y,z)(例如把 x 和 y 看成水平坐标, 而把 z 看成铅直坐标), 都附加一个向量 (u,v,w) 代表风在此点的速度, u,v 和 w 就是 x,y 和 z 方向的分速度.

现在取三个小数 h,k 和 l, 用它们来把点 (x,y,z) 稍稍变动一下, 再来看点 $(x+h,y+k,z+l)$. 我们希望, 在这个新点上风速向量也稍有变化, 成为 $(u+p,v+q,w+r)$. 风速的微小变化 (p,q,r) 怎样依赖于位置向量的微小变化 (h,k,l) 呢? 只要风不那么像湍流, 而 h,k 和 l 又足够小, 我们希望这种依赖性大体上是线性的, 自然界就是如此行事的. 换句话说, 我们希望有某个线性映射 T, 使得当 h,k 和 l 足够小的时候, (p,q,r) 大体上就是 (h,k,l), 注意, (p,q,r) 的每一个都依赖于所有的 h,k,l, 所以就需要 9 个数才能确定这个线性映射. 事实上, 我们可以把这个线性映射写成矩阵形式:

$$\begin{pmatrix} p \\ q \\ r \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \begin{pmatrix} h \\ k \\ l \end{pmatrix}.$$

矩阵的各个项 a_{ij} 就表示各个依赖性. 例如, 若 x 和 z 是固定的, 也就是若 $h=l=0$, 由此可知 a_{12} 就是分量 u 在只有 y 变动时的变率. 就是说, a_{12} 是 (x,y,z) 点处的偏导数 $\partial u/\partial y$.

这样就算出了矩阵, 但是从思想观念来看, 采用向量记号更加方便. 用黑体的字母 $\boldsymbol{x}$ 来表示 (x,y,z), 类似地, 用黑体 $\boldsymbol{u}(\boldsymbol{x})$ 代表 (u,v,w), 黑体 $\boldsymbol{h}$ 代表 (h,k,l), 黑体 $\boldsymbol{p}$ 代表 (p,q,r). 于是我们所说的就是对于某个比较 $\boldsymbol{h}$ 更小的向量 $\varepsilon(\boldsymbol{h})$, 有

$$\boldsymbol{p} = T(\boldsymbol{h}) + \varepsilon(\boldsymbol{h}).$$

换一个说法, 我们可以写出

$$\boldsymbol{u}(\boldsymbol{x}+\boldsymbol{h}) = \boldsymbol{u}(\boldsymbol{x}) + T(\boldsymbol{h}) + \varepsilon(\boldsymbol{h}),$$

这是一个与前面的公式 $g(x+h)=g(x)+mh+\varepsilon(h)$ 非常相似的公式. 它告诉我们, 如果对 $\boldsymbol{x}$ 加上一个很小的向量 $\boldsymbol{h}$, 则 $\boldsymbol{u}(\boldsymbol{x})$ 的改变大体就是 $T(\boldsymbol{h})$.

更一般地说, 令 $\boldsymbol{u}$ 是一个从 $\mathbf{R}^n$ 到 $\mathbf{R}^m$ 的函数. 如果存在一个从 $\mathbf{R}^n$ 到 $\mathbf{R}^m$ 的线性映射 $T:\mathbf{R}^n\to\mathbf{R}^m$ 使得公式

$$\boldsymbol{u}(\boldsymbol{x}+\boldsymbol{h})=\boldsymbol{u}(\boldsymbol{x})+T(\boldsymbol{h})+\varepsilon(\boldsymbol{h})$$

成立, 其中 $\varepsilon(\boldsymbol{h})$ 是一个相对于 $\boldsymbol{h}$ 更小的向量, 则定义 $\boldsymbol{u}$ 在点 $\boldsymbol{x}\in\mathbf{R}^n$ 处可微. 线性映射 T 称为 $\boldsymbol{u}$ 在 $\boldsymbol{x}$ 点的导数.

$m=1$ 时是一个重要的特例. 若 $f:\mathbf{R}^n\to\mathbf{R}$ 在 $\boldsymbol{x}$ 点可微, 则 f 在 $\boldsymbol{x}$ 处的导数是一个从 $\mathbf{R}^n$ 到 $\mathbf{R}$ 的一个线性映射 T. 这时, T 的矩阵是一个长度为 n 的列向量, 它时常记作 $\nabla f(\boldsymbol{x})$, 并称为 f 在 $\boldsymbol{x}$ 处的梯度. 这个向量指向 f 增长最快的方向, 其大小就是 f 在这个方向上的变率.

5.4 偏微分方程

偏微分方程在物理学中具有极大的重要性, 而且曾经启发出了大量的数学研究. 这里要讨论三个基本的例子, 作为本书以后更高深的条目的引导 (见偏微分方程[IV.12]).

第一个例子是热方程, 顾名思义, 它描述热在一个物理介质里的分布怎样随时间变化, 这时会得到下面的方程:

$$\frac{\partial T}{\partial t}=\kappa\left(\frac{\partial^2 T}{\partial x^2}+\frac{\partial^2 T}{\partial y^2}+\frac{\partial^2 T}{\partial z^2}\right),$$

这里, $T(x,y,z,t)$ 刻画位于 (x,y,z) 处在时刻 t 的温度.

学会读一个这样的方程, 并且懂得构成它的那些符号, 这是一回事, 但是能够看出它到底表示什么, 则是颇不相同的另一件事. 然而, 做到这一点是很重要的, 因为在我们能够写出的含有偏导数的许许多多表达式中, 只有少数几个很有意义, 它们时常有有趣的解释. 所以, 让我们来试着解释出现在热方程里的表达式.

左方的 $\dfrac{\partial T}{\partial t}$ 很简单, 就是令空间坐标 x,y 和 z 不动而时间 t 变化时, 温度 $T(x,y,z,t)$ 的变率. 换句话说, 它告诉我们, 在 (x,y,z) 点, 在时刻 t, 介质多么快地变热或者变冷. 我们希望这个变率依赖于什么? 热在介质里面旅行是需要时间的, 虽然在远处 (x',y',z') 点的温度终究会影响到 (x,y,z) 点的温度, 但是温度正在变化的方式只会受到近于 (x,y,z) 点的地方的温度的影响, 如果就在 (x,y,z) 的紧接着的近邻, 介质温度平均地比在此点热一点, 我们就会预期到温度上升, 如果冷一点, 就预期会下降.

右方括弧里的式子出现得那么频繁, 所以它自己也有一个简写的符号 Δ, 定义为

$$\Delta f = \frac{\partial^2 f}{\partial x^2} + \frac{\partial^2 f}{\partial y^2} + \frac{\partial^2 f}{\partial z^2},$$

称为拉普拉斯算子. 那么, Δf 关于函数 f 提供了什么信息呢? 答案是: 它正好包含了上一段说到的思想, 它告诉我们当这个邻域的大小趋于零时, f 在 (x, y, z) 点的值与它在 (x, y, z) 点的紧接着的邻域里的平均值的比较.

这一点从公式看并不明显, 但是下面的一维情况的论证 (虽然不太严密) 却给出为什么会有二阶导数出现的线索. 令 f 是一个把实数变成实数的函数. 为了得到 f 在 x 点的二阶导数的一个好的近似, 我们来对小的 h 看以下的表达式: $(f'(x) - f'(x-h))/h$(如果把 h 换成 $-h$, 会得到比较常见的公式, 但是这一个在这里更加方便). 导数 $f'(x)$ 和 $f'(x-h)$ 本身又可以分别用 $(f(x+h) - f(x))/h$ 和 $(f(x) - f(x-h))/h$ 来逼近, 把这些近似的式子都代入早前的表达式, 就会得到

$$\frac{1}{h}\left(\frac{f(x+h) - f(x)}{h} - \frac{f(x) - f(x-h)}{h}\right),$$

它就等于 $(f(x+h) - 2f(x) + f(x-h))/h^2$, 把它的分子除以 2, 就得到 $\frac{1}{2}(f(x+h) + f(x-h)) - f(x)$, 这就是 f 在 x 点的值与它在两个邻近点 $x+h$ 和 $x-h$ 的平均值的差.

换句话说, 二阶导数传递的正是我们需要的思想 —— 在 x 点的值和在 x 的附近的平均值的比较. 值得注意的是, 如果 f 是线性的, 则 $f(x-h)$ 和 $f(x+h)$ 的平均值就等于 $f(x)$, 这与我们熟知的事实, 即线性函数 f 的二阶导数为零是相符合的.

正如我们在定义一阶导数时要用 h 去除 $f(x+h) - f(x)$, 使得分子 $f(x+h) - f(x)$ 不仅自身变得很小 [而且与 h 的比值有极限], 所以, 对于二阶导数, 用 h^2 去除是适当的 (这也是合乎情理的, 因为一阶导数关系到线性逼近, 二阶导数关系到二次逼近, 准确地说, 对于函数 f, 在 x 点附近, 最好的二次近似就是 $f(x+h) \approx f(x) + hf'(x) + \frac{1}{2}h^2 f''(x)$, 而如果从一开始 f 就是一个二次函数, 可以验证, 这个近似式变成了准确的).

可以追随这类思想来证明, 如果 f 是三个变量的函数, 则 Δf 在 (x, y, z) 处的值确实告诉我们 f 在 (x, y, z) 处的值与它在 (x, y, z) 附近的平均值的比较如何 (自变量的个数 3 在这里没有什么特别 —— 这里的思想很容易推广到任意多个变量的函数). 在热方程里, 余下需要讨论的就是参数 κ 了, 它量度介质的导热性. 如果 κ 很小, 则介质传热性不好, 而 ΔT 对温度的变率的效应也比较小; 若它大一点, 热就传导得好一点, 效应也就大一点.

第二个具有很大重要性的方程是拉普拉斯方程 $\Delta f=0$. 直观地看, 它说的是, 一个函数 f 在一点 (x,y,z) 的值总是等于它在紧接着的周围的平均值. 如果 f 是一个变量 x 的函数, 这个方程说的就是 f 的二阶导数为零, 这蕴含着 f 的形状是 $ax+b$. 然而, 如果 f 是两个或更多个变量的函数, 情况就要灵活多变得多 —— 这函数在某些方向上, 可以位于切线上方, 而在另一些方向上则位于切线下方. 结果是, 我们可以对 f 赋予多种边值条件 (就是在某个区域的边界上指定 f 的值), 而且这会有大得多也更加有趣的解的类.

第三个基本的方程是波方程. 它的一维情况的陈述是：它描述连接两点 A 与 B 的振动的弦的运动. 设用 $h(x,t)$ 来记弦在距离 A 为 x 处、时刻 t 时的高度. 波方程指出

$$\frac{1}{v^2}\frac{\partial^2 h}{\partial t^2}=\frac{\partial^2 h}{\partial x^2}.$$

暂时不去管常数 $1/v^2$, 方程左方表示弦在离开 A 点为 x 处的一小段的 (铅直方向的) 加速度. 这个加速度应该正比于作用于弦的这一小段的力. 那么, 是什么来决定这个力呢？暂时设弦的包含 x 的一小段是直的, 则从 x 左方来的对弦的拉力与来自 x 右方的拉力就完全抵消了, 而作用的净力为零. 这样, 问题又一次成了 x 处弦的高度与邻近的高度平均值的比较, 如果弦位于 x 处的切线的上方, 就应该有一个向上的力, 如果弦在下方, 就应有向下的力. 这就是为什么二阶导数又一次出现在方程右方. 由这个二阶导数到底能得出多大的力取决于以下因素, 例如弦的密度和拉紧的程度, 这样在右方就出现了一个常数. 因为 h 和 x 都是距离, v^2 就有 (距离/时间)^2 的量纲, 这就意味着 v 是一个速度, 事实上, 它就是波传播的速度.

类似地, 考虑可以给出三维的波方程, 我们可以想象到, 它应该是

$$\frac{1}{v^2}\frac{\partial^2 h}{\partial t^2}=\frac{\partial^2 h}{\partial x^2}+\frac{\partial^2 h}{\partial y^2}+\frac{\partial^2 h}{\partial z^2},$$

或简单一些写为

$$\frac{1}{v^2}\frac{\partial^2 h}{\partial t^2}=\Delta h.$$

还可以把它写得更简单一些, 即 $\square=0$, 这里, $\square$ 是

$$\Delta h-\frac{1}{v^2}\frac{\partial^2 h}{\partial t^2}$$

的简写. 算子 $\square$ 称为达朗贝尔算子, 这是根据法国数学家达朗贝尔[VI.20] 命名的.

5.5 积分

设有一辆汽车沿直路行驶 1 分钟, 并且给出汽车的起点在哪里, 这 1 分钟内的速度又是多少, 能不能说出车走了多远？如果在整个这 1 分钟内, 速度都是相同的,

则问题很简单 —— 例如, 设车速是每小时 30 英里, 只要把车速除以 60, 就知道它走了半英里 —— 但是, 若车速是在变化的, 问题就比较有趣了. 这时, 我们不再试图给出准确的答案, 而是用下面的技巧去逼近它. 首先, 给出汽车在这 60 秒的每一秒开始时的速度. 其次, 在每一秒内做一个简单的计算, 看看汽车在这 1 秒之内走了多远. 这个技巧就是假设汽车的速度在整个 1 秒钟之内都等于它在 1 秒钟之始的速度. 最后, 把这些距离加起来. 因为 1 秒钟只是很短的一段时间, 在这 1 秒钟之内汽车的速度变化不会大, 所以这个程序会给出相当准确的答案. 再说, 如果还不满意于其准确度, 还可以把 1 分钟分成更短的时间段.

如果您读过一门初等的微积分课程, 就会用一种完全不同的方法来解决这个问题了. 在一个典型的问题里, 会给出速度在时刻 t 的显示公式 —— 例如 $at+u$ 之类 —— 要想算出汽车走了多远, 只需要把这个函数 "积分" 出来, 就得到在时刻 t 已经走过的距离是 $\frac{1}{2}at^2+ut$. 这里的所谓积分就是微分的反运算: 要找出函数 $f(t)$ 的积分, 就是要找一个函数 $g(t)$ 使得 $g'(t)=f(t)$. 这样做确实是有理由的, 因为如果 $g(t)$ 是走过的距离, 而 $f(t)$ 是速度, 那么, $f(t)$ 就是 $g(t)$ 的变化率.

然而, 反导数并不是积分的定义. 要想看出为什么不是, 考虑下面的例子. 如果在时刻 t 速度是 e^{-t^2}, 那么走过的距离是多少? 大家知道, 没有一个 "好" 的函数 (粗略地说, 所谓好函数, 就是从诸如多项式、指数、对数、三角函数之类的标准的函数 "构建" 起来的函数) 是以 e^{-t^2} 为其导数的, 然而这个问题确实是有意义的而且有确定的解答 (您很可能听说过有这样的函数 $\Phi(t)$ 求导以后给出 $\mathrm{e}^{-t^2/2}$, 由它可知, $\Phi(t\sqrt{2})/\sqrt{2}$ 微分以后就给出 e^{-t^2}. 然而这并没有回答我们的问题, 因为 $\Phi(t)$ 是定义为 $\mathrm{e}^{-t^2/2}$ 的积分的 [怎样求它, 仍然还是问题]).

为了在这种反导数遇到困难时也能定义积分, 我们又得回到前面讨论过的那种令人糊涂的逼近过程. 沿这条思路的一个形式定义是由黎曼[VI.49] 在 19 世纪中叶给出的. 为了看清黎曼的基本思想何在, 以及看清积分和微分一样, 可以很有用地用于多于一个变量的函数, 我们来看另一个物理问题.

设有一块质地不纯的石头, 想要从它的密度来算出它的质量. 又设密度并非常值的, 而在整块石头内可以很不规则地变化, 甚至石头里面可能有洞, 所以在洞的那些地方密度为零. 该怎么办?

黎曼的途径是这样的. 第一步, 把石头放在一个立方体里面. 对于立方体的每一点 (x,y,z) 都有密度值 $d(x,y,z)$(如果点 (x,y,z) 取在石头外部, 或在一个洞里, 就令密度为零). 第二步, 把这个立方体分成许许多多的小立方体. 第三步, 在每一个小立方体里, 找出密度最低的点 (如果这样的点在石头外部, 或在一个洞里, 就令这个最低的密度值为零), 也找出密度最高的点. 令 C 为一个小立方体, 而设其中密度的最小与最大值分别为 a 和 b, C 的体积则为 V, 这时, 石头的 C 这一部分的

质量必在 aV 和 bV 之间. 第四步, 把这样得到的 aV 加起来, 也把这些 bV 加起来. 如果总和为 M_1 和 M_2, 则石头的总质量就在 M_1 和 M_2 之间. 第五步, 把小立方体分得越来越小, 并且重复上面的计算. 这样做的时候, M_1 和 M_2 就会变得越来越接近, 也就得到了石头质量的越来越好的近似.

类似于此, [如果让黎曼来处理汽车问题, 他也会] 把这 1 分钟的时间分成小区间, 并且在这些小区间里找出对于每一个小区间的最小与最大速度, 就会得到一对数 a 和 b, 于是就可以说, 汽车在这一小段时间里的旅程最少是 a, 而最多是 b. 把这样两组数加起来, 就可以说, 在整个 1 分钟时间里, 汽车走过的距离至少是 D_1(就是 a 的和), 而最多是 D_2(就是 b 的和).

在这两个问题里, 我们都有一个函数 (密度/速度), 定义在一个集合 (立方体/1 分钟) 上, 要求出这个函数在某种意义下的 "总量". 我们的做法都是把这个集合分成小的部分, 而在这些小部分里都用简单的计算, 得出这个量的下方与上方的近似. 这个程序就以 (黎曼) 积分 [方法] 而闻名于世. 下面的记号是常用的. 若 S 表示这个集合, f 表示这个函数, 于是 f 在 S 上的总量, 就叫做 f 在 S 上的积分 [更准确些, 叫做黎曼积分], 并且写作 $\int_S f(x)\mathrm{d}x$. 这里用 x 记 S 的一个典型的元素. 如果在密度的例子里 S 的元素是点 (x, y, z), 则可以用 $\int_S f(x)\mathrm{d}x$ 这样的向量记号, 虽然并不常用, 读者可以从上下文分清 "x" 现在是代表向量, 还是通常的实数.

我们花了不少功夫来把积分和反导数区分开来, 但是有一个称为微积分基本定理的著名定理, 断言这两个程序事实上会给出相同的答案, 至少当所考察的函数具有所有的 "合理的" 函数一定会具有的某些连续性时是这样的. 所以, 通常都认为把积分看成微分的反运算是合法的. 确切些说, 如果 f 是连续的, 而 $F(x)$ 可以对于某个常数 a 定义为 $F(x) = \int_a^x f(t)\mathrm{d}t$, 则 $F(x)$ 可以微分, 而且 $F'(x) = f(x)$. 就是说, 如果先把一个连续函数积分了, 再去做微分, 就会回到原来的函数. 反过来说, 如果 F 有连续导数 f, [而 a 是一个适当选取的数]①, 则 $\int_a^x f(t)\mathrm{d}t = F(x) - F(a)$. 这几乎就是说如果先把 F 微分了, 然后再取积分, 就又会回到 F. 事实上, 需要选取一个任意的常数 a, 而得到的是函数 F 减去 $F(a)$.

如果不假设连续性, 那么会得到什么样的例外, 看一下所谓的赫维赛德 (Heaviside) 阶梯函数 $H(x)$ 的例子, 就会有一点概念了. 当 $x < 0$ 时这个函数为 0, 而当 $x \geqslant 0$ 时为 1. 它在 $x = 0$ 处有一个跳跃, 所以在那里是不连续的. 当 $x < 0$ 时这个函数的积分 $J(x)$ 为 0, 而当 $x \geqslant 0$ 时为 x. 对于几乎所有的 x 值, 有 $J'(x) = H(x)$. 然而 $J(x)$ 的梯度在 0 处会突然跳跃, 所以 J 在那里是不可微的, 而不能说 $J'(0) = H(0) = 1$.

---

① 原书误为 "$a < x$".—— 中译本注

5.6　全纯函数

数学王冠上有一颗宝石, 就是复分析, 它研究的就是变数为复数的可微函数. 这一类函数称为全纯函数.

这些函数一开始看来并没有什么特别的地方, 因为在这个情况下, 导数的定义也与实变量函数的导数定义一样: 若 f 是一个函数, 它在复数 z 处的导数定义也是当 h 趋于零时 $(f(z+h)-f(z))/h$ 的极限. 然而, 如果以稍微不同的方式 (就是在 §5.3 里看到的方式) 来看这个定义就会发现, 想要一个复 [自变量] 的函数可微并不那么容易. 回想一下, 在 §5 里面说过, 微分就是线性逼近. 在复函数① 情况下这就是说, 我们想用形为 $g(w)=\lambda w+\mu$ 的函数去逼近 $f(w)$, 这里 λ,μ 都是复数 (在 z 点附近, $f(w)$ 的这个逼近式就是 $g(w)=f(z)+f'(z)(w-z)$, 所以 $\lambda=f'(z),\mu=f(z)$).

让我们从几何上来看待这里的情况. 如果 $\lambda\neq 0$, 则对 $(w-z)$ 乘以 λ 就相当于把它按照某个因子 $r=|\lambda|=|f'(z)|$ 将 $(w-z)$ 缩放, 再将它旋转一个角 $\theta=\arg\lambda$. 这意味着许多通常被认为是平面上的线性变换, 例如反射、剪切、各方向不同的拉伸等等, 现在都被排除了. 为了确定 λ, 只需要两个实数 (不论是把 λ 写为 $a+b\mathrm{i}$ 还是写为 $re^{\mathrm{i}\theta}$ 都是这样), 但是要确定平面上的一般的线性变换则需要四个 (见 §4.2 中关于矩阵的讨论). 这种自由度数目的减少将用一组称为柯西–黎曼方程的微分方程来表示. 我们不再写 $f(z)$ 而把它写为 $u(x+\mathrm{i}y)+\mathrm{i}v(x+\mathrm{i}y)$, 这里 x,y 分别是 z 的实部和虚部, $u(x+\mathrm{i}y),v(x+\mathrm{i}y)$ 则是 $f(z)$ 的实部和虚部. 于是 f 在 z 点附近的线性逼近具有以下的矩阵:

$$\begin{pmatrix} \dfrac{\partial u}{\partial x} & \dfrac{\partial u}{\partial y} \\ \dfrac{\partial v}{\partial x} & \dfrac{\partial v}{\partial y} \end{pmatrix}.$$

缩放和旋转的矩阵形状是 $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, 将它与上面的矩阵比较, 就得到所谓的柯西 — 黎曼方程

$$\frac{\partial u}{\partial x}=\frac{\partial v}{\partial y},\quad \frac{\partial u}{\partial y}=-\frac{\partial v}{\partial x}.$$

它的一个推论就是

$$\frac{\partial^2 u}{\partial x^2}+\frac{\partial^2 u}{\partial y^2}=\frac{\partial^2 v}{\partial x\partial y}-\frac{\partial^2 v}{\partial y\partial x}=0$$

(并不清楚混合偏导数的对称性是否作为必要条件而成立, 但是对于全纯函数, 它是成立的). 所以 u 适合拉普拉斯方程 (这个方程在 §5.4 中讨论过). 类似的论证表明 v 也是如此.

① 对于所谓 "复函数", 需要区别是指自变量为复还是函数值为复. 当自变量为复数时, 情况与实自变量完全不同. 所以, 如果没有特别说明, 本节里的复函数都是指的复自变量的函数. —— 中译本注

这些事实开始向我们建议, 复的可微性是一个比实的可微性强得多的条件, 所以可以预期, 全纯函数会有许多有趣的性质. 现在让我们来看一下它们确实具有的值得注意的几个性质.

第一, 关于微积分基本定理 (在前一节讨论过). 设 F 是一个全纯函数, 而已知其导数 f 和 F 在某个复数 u 处的值, 怎样把 F 重新构造出来? 一个近似的方法如下: 令 w 为另一个复数, 我们想把 $F(w)$ 做出来. 取一串点 $z_0, z_1, \cdots, z_n$, 其中 $z_0 = u$, 而 $z_n = w$. 设所有的差 $|z_1 - z_0|, |z_2 - z_1|, \cdots, |z_n - z_{n-1}|$ 都很小. 我们可以用 $(z_{i+1} - z_i)f(z_i)$ 来逼近 $F(z_{i+1}) - F(z_i)$. 由此可知 $F(w) - F(u) = F(z_n) - F(z_0)$ 可以用 $(z_{i+1} - z_i)f(z_i)$ 之和来逼近 (因为我们把许多小的误差都加到一起来了, 这个逼近是不是很好就不明显了, 但是结果是它仍然是一个好的逼近). 我们可以想象一个复数 u 从 z 点开始, 沿着一条从 z 到 w 的路径 P, 从分点 z_i 跳一小步 $\delta z = z_{i+1} - z_i$ 到另一个分点 z_{i+1}, 一直跳到 w. 当 n 趋向无穷, 而每一步的步长 δz 都趋向零时, 就会得到一个所谓的路径积分, 记作 $\int_P f(z)\mathrm{d}z$. [由此得到复情况下的微积分基本定理: 如果 f 是全纯函数 F 的导数, 则有 $F(w) - F(z) = \int_P f(z)\mathrm{d}z$].

由上面的论证可以得到一个推论: 若路径 P 从点 z 又回到同一点, 则路径积分为零, $\int_P f(z)\mathrm{d}z = 0$[就是说, 如果 f 是全纯函数 F 的导数, 则它在任意闭路径上的积分为零]. 与此等价有: 若两条路径 P_1 和 P_2 有相同的起点 z 和相同的终点 w, 则路径积分 $\int_{P_1} f(z)\mathrm{d}z$ 和 $\int_{P_2} f(z)\mathrm{d}z$ 相等, 因为它们都等于 $F(w) - F(z)$[这时, 我们说如果 f 是全纯函数 F 的导数, 则它的积分值与积分路径无关][①].

[所有这些结果都是在一个大的假设: f 是全纯函数 F 的导数下才得到证明的. 问题在于如果我们不是假设 f 是某个全纯函数 F 的导数, 而是假设它本身就是一个全纯函数, 以上结果是否仍然成立? 复分析里一个可以说是最重要的定理 —— 柯西定理 —— 告诉我们, 这些结果仍然成立. 具体说, (1) 如果 f 是一个全纯函数, 则在任意的闭积分路径 P 上, $\int_P f(z)\mathrm{d}z = 0$, 或者说, (2) 如果 f 是一个全纯函数, 则它的积分值与积分路径无关. 这时, 任意取一条由 z 到 w 的路径 P, 其上的积分 $\int_P f(z)\mathrm{d}z$ 就可以记为 $\int_z^w f(z)\mathrm{d}z$, 它就是 w 的函数 F(但可能相差一个常数), 而 f 就是它的导数, $F' = f$. 这就是说, 不必要求 f 是某个全纯函数 F 的导数, 只需要求它自己有导数, 因此是全纯函数就行了. 这时上面的积分 $\int_z^w f(z)\mathrm{d}z$ 就是它的反导数. 所以, 一个有导数 (即可微) 的复函数, 自动地就有反导数].

为了使以上所说的这些结果成立, 并不需要 f 定义在整个复数平面 $\mathbf{C}$ 上, 如

① 由于这里的结论极为重要, 而本书的讲法与国内读者的习惯又不太一致, 所以译者作了一些文字的修改或补充, 这些修改与补充都放在方括号里.—— 中译本注

果限制 f 定义在整个复数平面的一个单连通区域, 即没有洞的开集合[III.90]上, 则以上的一切都成立. 如果区域里有洞, 则在两条有相同起点和终点的路径上的积分, 当这两个路径合起来包围了洞时, 这两个积分的值可以相差一个常数. 因此, 路径积分与平面的子集合的拓扑学有密切的关系, 这一点观察在整个现代几何学里面有繁茂的衍生物. 关于拓扑学, 可以进一步参看 §6.4 和代数拓扑[IV.6] 这一条目.

可以从柯西定理推导出一件惊人的事情, 即若 f 是全纯的, 它一定可以微分两次 (对于实值函数, 这是完全不真的, 例如考虑这样的函数 f, 当 $x < 0$ 时, 定义 $f(x) = 0$, 而当 $x \geqslant 0$ 时, 定义 $f(x) = x^2$, 这个函数在 $x = 0$ 处就不能微分两次). 由此可得 f' 也是全纯函数, 所以也可以微分两次. 继续下去, 就知道 f 可以微分任意次. 这样, 对于复函数, 可微性蕴含无穷可微性 (前面说到过的混合偏导数的对称性, 甚至存在性, 都可以由此导出).

一个密切相关的事实是, 只要一个全纯函数有了定义, 就一定能够展开为幂级数. 就是说, 如果 f 定义在以 w 为中心、R 为半径的开圆盘上, 而且在那里可微, 它就一定可以表示为

$$f(z) = \sum_{n=0}^{\infty} a_n(z-w)^n,$$

这个级数在这个圆盘中处处有效, 即在此圆盘中收敛. 这个幂级数称为 f 的泰勒展开式.

全纯函数的另一个基本的性质是它的全部性态可以由它在一个小区域里的性态完全决定. 这个性质说明了它们是何等地具有 “刚性”. 由此, 如果 f 和 g 都是全纯的, 而且它们在某个小圆盘内取相同的值, 则它们必定有相同的定义域而且处处取相同值. 这个值得注意的事实允许定义一种所谓解析拓展的过程: 如果在想要定义一个全纯函数的整个区域上去定义它有困难, 那么只需简单地在某个小区域里定义它, 然后就可以说, 它处处都只能取与已经确定的值相容的唯一的值. 著名的黎曼 ζ 函数[IV.2§3] 通常就是这样定义的.

最后我们还要提到刘维尔[VI.39] 的一个定理, 这个定理说, 如果 f 是定义在整个复平面上的全纯函数, 而且 f 是有界的 (即存在一个常数 C, 使得对于每一个复数 z 都有 $|f(z)| \leqslant C$), 则 f 必为常数. 例如, 函数 $\sin x$ 对于实的 x, 毫无困难地把有界性与极好的性质连在一起: 它可以展开为一个处处收敛的幂级数 (然而, 如果用这个幂级数把 $\sin x$ 拓展到复平面上, 则如刘维尔定理所预期到的一样, 所得到的函数就不再是有界的了).

6. 什么是几何学

在本文中想要对几何学作一个恰当的处理是不容易的. 因为这个分支的基本概念要么太简单, 无需解释, 例如, 没有必要在这里来讲什么是圆, 什么是直线, 什

么是平面等等; 要么就比较高深, 放到本书的第III、第IV部分去讨论更好. 然而, 如果没有见过这些高深的概念, 对于现代几何学将一无所知, 那么, 要是懂得了两个基本概念, 从本书的收获一定会大得多. 这两个概念就是: 几何学与对称性的关系, 以及流形的概念. 本节就将致力于讨论它们.

6.1 几何学与对称群

广泛地说, 几何学就是数学里使用通常都约定是几何语言的那一部分, 在那里, 诸如 "点""直线""平面""空间""曲线""球""立方体""距离", 还有 "角", 这些词起了卓越的作用. 但是, 还有一个更深刻的观点, 就是克莱因[VI.57] 所主张的观点, 认为变换才是这门学科的真正主题. 所以, 除了上面列举的那些词以外, 还要加上 "反射""旋转""平移""拉伸""剪切" 和 "投影" 这些词, 还有稍微不太清楚的概念, 例如 "保角映射" 或者 "连续变形".

在 §2.1 中就讨论过, 变换总是和群在一起, 因为这个原因, 几何学与群论就有密切的关系. 说真的, 给定了一个变换群, 就有一种相应的几何学. 在这种几何学里研究的就是那些不受这个群的变换影响的现象. 特别是, 若一个图形经过此群中的一个变换能够变成另一个图形, 就说它们是等价的. 不同的群当然会导出不同的等价概念, 因此数学家们时常谈论到各种几何学, 而不是把几何学当作一门铁板一块的单个学科. 这一节就要简短地描述一下最重要的几何学以及与之相关的变换群.

6.2 欧几里得几何学

欧几里得几何 (简称欧氏几何) 就是绝大多数人想的 "普通的几何学", 它有这么个名字也不奇怪, 因为它包括了希腊几何学的基本定理, 而希腊几何学家们是两千多年来的几何学家的主体. [欧几里得是最著名的希腊几何学家的代表人物, 所以, 人们就把希腊几何学称为欧几里得几何学]. 例如, 三角形的内角和为 180° 这个定理就属于欧几里得几何学.

要想从变换的角度来看待欧几里得几何, 就先要说明是在多少维的空间里进行研究的, 当然也必须指定一个变换群. 适当的变换就是刚性变换. 可以用两个方法来考虑这种变换. 其一是, 刚性变换就是在平面里、三维空间里, 或者更为一般是在 $\mathbf{R}^n$(n 是一个正整数) 里的保持距离不变的变换. 就是说, 给定两个点 x 与 y, 若一个变换 T 使得 Tx 和 Ty 的距离等于 x 和 y 的距离, 就说 T 是一个刚性变换 (如果维数大于 3, 距离将以一种推广毕达哥拉斯公式的方式自然地定义. 详见度量空间[III.56]).

后来发现, 每一个这样的变换都可以用旋转、反射和平移的复合来实现. 这就给了第二种也是比较具体的思考这个群的方法. 换句话说, 欧几里得几何研究的就是那些在旋转、反射和平移下不变的概念, 这些概念里就包括了点、直线、平面、

圆、球、距离、角、长度、面积和体积. $\mathbf{R}^n$ 中的旋转构成了一个重要的群: 特殊正交群, 记作 $\mathrm{SO}(n)$. 更大一点的正交群 $O(n)$ 还把反射也包括进去了 (在 n 维空间里怎样定义旋转, 并不太显然, 但是不算太难. $\mathbf{R}^n$ 中的正交映射就是一个保持距离的线性映射 T, 即是使得 $d(Tx, Ty) = d(x, y)$ 的映射. 如果它的行列式[III.15] 为 $+1$, 它就是一个旋转. 保持距离的映射的行列式唯一可取的其他值就是 -1. 行列式为 -1 的映射在 "把里面翻到外面来" 这一点上, 就像是反射).

6.3 仿射几何学

除了旋转和反射以外还有许多别的线性映射. 如果把 $\mathrm{SO}(n)$ 或者 $O(n)$ 放大, 使之把尽可能多的这些线性变换也包括进来, 又会发生什么? 要使一个变换成为群的元素, 它就必须是可逆的, 但并非所有线性变换都是如此, 所以一个自然的应该考察的群就是由 $\mathbf{R}^n$ 的所有可逆的线性变换所成的群 $\mathrm{GL}_n(R)$, 这个群我们已经在 §4.2 中见到过了. 所有这些变换都令原点不动. 但如果我们愿意, 还可以把平移也加进来得到一个更大的群, 就是包括所有形如 $x \mapsto Tx + b$ 的变换所成的群. 这里 b 是一个固定的向量, 而 T 是一个可逆的线性变换. 这样得到的几何学称为仿射几何学.

因为线性映射中还包括了拉伸和剪切, 它们既不能保持距离也不能保持角度, 所以距离和角度都不是仿射几何学的概念. 然而, 经过可逆的线性映射和平移以后, 点、直线、平面仍然是点、直线、平面, 所以这些概念都属于仿射几何学. 另一个仿射概念是两条直线的平行 (就是说, 虽然线性映射一般并不保持角度不变, 但是, 角度为零却得到了保持). 这意味着虽然在仿射几何学中没有矩形或正方形这样的东西, 却可以讨论平行四边形. 类似地, 虽然不能讨论圆, 却可以讨论椭圆, 因为线性映射总是把椭圆变为椭圆 (当然, 这里要把圆看作椭圆的特例).

6.4 拓扑学

与一个群相联系的几何学 "研究的是被此群的所有变换保持的概念" 这个思想可以用等价关系[I.2 §2.3] 搞得更加确切. 事实上, 令 G 是 $\mathbf{R}^n$ 中的一个变换群. 可以把一个 d 维 "图形" 看成是 $\mathbf{R}^n$ 的一个子集合 S. 在研究 G 几何学的时候, 并不把 S 和从它经过 G 中的变换得来的集合相区别. 所以这时我们说这两个图形是等价的. 例如, 两个图形在欧几里得几何中为等价, 当且仅当它们在通常的意义下是全等的, 而在二维仿射几何学里, 所有的平行四边形都是等价的, 所有的椭圆也都是等价的. 总之, 我们可以认为 G 几何学的基本对象是图形的等价类, 而不是图形本身.

拓扑学可以认为是当应用最宽松的等价概念所得到的几何学, 其中我们说两个图形是等价的, 或者用数学语言说是同胚的, 如果二者的每一个都可以 "连续变形"

为另一个. 例如, 球和立方体就是在这个意义下等价的, 如图 1 所示.

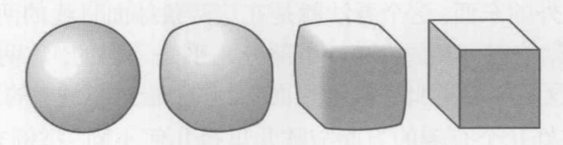


图 1 球变形成了立方体

因为存在很多很多的连续变形, 要想说两个图形在这个意义下不等价就很难了. 例如, 似乎很明显, 球面 (就是球体的表面, 而不是立体的球体) 不能连续变形为一个环面 (就是轮胎那种有洞的曲面的图形), 因为它们是本质不同的图形 —— 一个有 "洞", 一个没有. 然而, 把这种直观变成严格的论证并非易事. 关于这类问题, 更详细的可见*不变式*[I.4 §2.2]、*代数拓扑*[IV.6] 和*微分拓扑*[IV.7].

6.5 球面几何学

至此, 我们一直是在逐步放松对于两个图形为等价的要求, 允许越来越多的变换. 现在我们要再次收紧, 考虑球面几何学. 现在的宇宙不再是 $\mathbf{R}^n$ 而是 n 维球面 S^n, 即半径为 1 的 $(n+1)$ 维球体的表面, 或者用代数方法来表示, 即 $\mathbf{R}^{n+1}$ 中适合方程 $x_1^2+x_2^2+\cdots+x_n^2=1$ 的点 $(x_1,x_2,\cdots,x_{n+1})$ 的集合. 正如 3 维球体的表面是 2 维的一样, 这个集合则是 n 维的. 我们将只讨论 $n=2$ 的情况, 但是很容易推广到更大的 n.

现在适当的变换群是 SO(3), 它是由所有这样的旋转组成, 这些旋转的轴是经过原点的直线 (也可以允许反射而取 $O(3)$, 它们是球面 S^2 的对称; 在球面几何学里就这样来看待它们, 不把它们看成整个 $\mathbf{R}^3$ 中的变换).

在球面几何学中有意义的概念有直线、距离和角. 限制在球体表面上而又谈论直线, 这看起来有些奇怪, 但是, "球面直线" 并不是通常意义下的直线, 而是 S^2 用如下方法得出的子集合: 用一个通过原点 (球心) 的平面与 S^2 相交所成的子集合 (叫做大圆), 即半径为 1 的圆, 就是球面直线, 而在一个半径为 1 的球体内, 这是可能做出的最大的圆了 [所以, 称它为大圆是合理的].

大圆值得看成某种直线的重要理由还在于 S^2 上的两点 x,y 之间最短的路径就是大圆 [的劣弧], 当然, 路径要限制位于 S^2 上. 这也是一个有实际意义的限制, 在地球表面上两个相离的点之间最短的路程就不是直线, 因为这些直线将要深埋在地下几百英里的地方了.

两点 x 和 y 之间的距离定义为连接 x 和 y 而且完全位于 S^2 上的最短路径的长度 (如果 x 和 y 位于一条直径的两端, 则有无穷多这样的路径, 其长度都是 π, 所以这时 x 和 y 的距离是 π). 至于两条球面直线之间的角又如何定义? 球面直线是定义为一个平面与 S^2 的交线的, 所以两条球面直线的交角可以定义为这两个平面

在欧几里得几何学意义下的角. 还有一个从审美角度来看更加使人愉快的观点, 它完全不涉及球面以外的东西. 这个看法就是在这两条球面直线的两个交点之一处看交点的一个小邻域, 这时, 球面的这一小部分几乎是平坦的, 这两条直线也几乎是直的. 所以可以定义这个角即此 "极限平面" 上的 "极限直线" 的通常意义下的角.

球面几何学在好几个有趣的方面与欧几里得几何不同. 举例来看, 一个球面三角形的三个角加起来一定大于 $180°$, 事实上, 如果取以下的顶点: 第一个是北极, 第二个取在赤道上, 最后一个取在赤道上与第二个相距一象限的地方, 就会得到三个角都是直角的球面三角形. 三角形越小, 它就越平坦, 三个角的和就越接近 $180°$. 有一个优美的定理对这个角差给出准确的表达式: 转用弧度制, 若有一个球面三角形, 其三个角为 α, β 和 γ, 则此三角形的面积为 $\alpha+\beta+\gamma-\pi$, [这里设球面的半径为 1](例如, 上面那个三个角均为 $\dfrac{\pi}{2}$ 的球面三角形面积为 $\dfrac{\pi}{2}$. 这个结果是真的, 因为半径为 1 的球面面积是 4π, 而我们做的那个三角形的面积确实是全球面的八分之一).

6.6 双曲几何学

迄今, 参照着变换的某个集合, 即变换群, 来看几何学, 这一思想只不过是看待这个学科的一个有用的途径, 一个对看来是很不相同的各个侧面的统一的观点. 然而, 来到双曲几何学时, 变换的途径就是不可少的了, 其理由马上就来说明.

产生双曲几何学的变换群是二维的特殊射影线性群, 记作 $\mathrm{PSL}_2(\mathbf{R})$, 讲解这个群的方法之一如下: 特殊线性群 $\mathrm{SL}_2(\mathbf{R})$ 是所有的行列式[III.15] 为 1 的矩阵 $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ 的集合, 即适合关系式 $ad-bc=1$ 的这种矩阵的集合 (它们确实构成一个群, 因为如果两个矩阵的行列式均为 1, 则它们的乘积也如此). 为了让它成为 "射影的", 就令矩阵 A 等价于 $-A$, 例如, 矩阵 $\begin{pmatrix} 3 & -1 \\ -5 & 2 \end{pmatrix}$ 和 $\begin{pmatrix} -3 & 1 \\ 5 & -2 \end{pmatrix}$ 就是等价的.

为了从这个群得出一种几何学, 首先必须把它解释为某个 2 维点集合的变换群. 一旦做到了这一点, 就把这个 2 维点集合称为双曲几何学的一个模型. 微妙之处就在于双曲几何学没有一个看起来是最为自然的模型, 如球面是球面几何学的模型那样 (人们可能以为球面是球面几何学的唯一合理的模型, 但是这不是事实. 例如, 有一个自然的方法使 $\mathbf{R}^3$ 的一个旋转与附加了 "无穷远点" 的 $\mathbf{R}^2$ 的一个变换联系起来, 这样就使得可以用扩充的 $\mathbf{R}^2$ 作为球面几何学的一个模型). 双曲几何学的三个最常用的模型是半平面模型、圆盘模型和双曲面模型.

半平面模型是与群 $\mathrm{PSL}_2(\mathbf{R})$ 最直接联系的模型, 所需要的 2 维平面点集合是

复平面 $\mathbf{C}$ 的上半平面, 即所有复数 $z=x+\mathrm{i}y, y>0$ 的集合. 给定了矩阵 $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ 以后, 相应于此矩阵的变换就是把点 z 变为 $(az+b)/(cz+d)$ (注意, 如果把 a,b,c,d 改为其负值, 也会得到同样的变换). 条件 $ad-bc=1$ 是用于证明变换后的点仍然在上半平面上, 还用于证明这个变换是可逆的.

这里还没有做的是: 对于距离还什么也没有说. 正是在这种几何学里, 需要用群来 "生成" 几何学. 如果想要有一个从变换群角度看来是合理的距离概念, 那么重要的就是这种变换要保持这个距离不变. 就是说, 如果 T 是一个这样的变换, 而 z 和 w 两点在上半平面里, 则 [$T(z)$ 和 $T(w)$ 也在上半平面, 而且 $d(T(z),T(w))=d(z,w)$. 可以证明, 本质上恰好只有一种定义距离的方法具有这个性质, 用变换来 "生成" 的几何学就是这个意思 (我们当然可以用同一个数值因子, 例如 3, 去乘这个距离, [并以之为新的距离], 但是这好比不用 "米" 而用 "尺" 来量距离一样, "生成" 的几何学和原来的几何学并没有真正的不同).

这个距离有一些初看起来显得奇怪的性质. 例如, 一条典型的双曲直线的形状是端点在实轴上的半圆弧. 但是, 说它是半圆, 不过是从 $\mathbf{C}$ 上的欧几里得几何学的观点来看是半圆; 从双曲几何学的观点来看, 欧几里得几何学的直线是 "直" 的, 也同样奇怪. 两种距离的真正差别在于, 双曲距离和欧几里得距离比较起来, 越是接近实轴, 前者变得越大. 所以要从点 z 走到点 w, "绕道" 偏离实轴, 路程反而更短, 最佳的弯道就是沿着连接点 z 和点 w 而且与实轴成直角的半圆弧 (如果点 z 和点 w 位于同一条铅直线上, 就会得到一个 "蜕化的" 圆弧, 它就是一条铅直的直线). 和平坦的世界地图比较, 这件事也算不得是悖论, 平坦的世界地图包含了对于球面几何学的扭曲, 所以例如格陵兰就显得太大了. 半平面模型就是一个几何结构, 即双曲平面的地图, 所以它的 "形状" 和真实情况是很不相同的.

2 维双曲几何学的最著名的性质之一, 就是它是一种使得欧几里得平行线公设不成立的几何学. 就是说, 可以找到一条双曲直线 L 和其外一点 x, 使得过点 x 可以画出两条直线都不与 L 相交. 在适当解释后, 欧几里得几何学的所有其他公理在双曲几何学中都成立. 由此可知, 从那些公理是不可能推导出平行线公设的. 这个发现, 联系着*高斯*[VI.26]、*波尔约*[VI.34] 和*罗巴切夫斯基*[VI.31], 解决了一个困扰历代数学家两千多年的问题.

另一个性质补全了关于欧几里得三角形和球面三角形的内角和的性质. 有一个很自然的双曲面积概念, 具有顶角 α,β 和 γ 的双曲三角形的面积是 $\pi-\alpha-\beta-\gamma$. 所以在双曲平面上, $\alpha+\beta+\gamma$ 总小于 π, 而当三角形非常小的时候, 就几乎等于 π. 内角和的性质反映了以下的事实: 球面具有正的*曲率*[III.13], 欧几里得平面是 "平坦" 的 [即有零曲率, 而双曲平面则有负曲率. 这样, 双曲三角形、欧几里得三角形

和球面三角形的内角和分别小于、等于和大于 π; 其差与曲率成正比; 而这些空间的曲率也相应地为负、为零和为正. 上面说是"补全了"相应性质, 就是这个意思].

圆盘模型是庞加莱[VI.61] 在一个著名的瞬间, 在登上一辆公共汽车的时刻想出来的[①], 它的点集合就是 $\mathbf{C}$ 平面的开单位圆盘, 也就是模小于 1 的复数的集合 D. 现在, 典型的变换形状如下. 取 D 中的一个复数 a 以及实数 θ, 这个变换就把 z 点变为点 $\mathrm{e}^{\mathrm{i}\theta}(z-a)/(1-\bar{a}z)$. 这些变换成为一个群并不完全是显然的, 而这个群同构于 $\mathrm{PSL}_2(\mathbf{R})$ 就更不显然. 然而可以证明, 变 z 为 $-(\mathrm{i}z+1)/(z+\mathrm{i})$ 的函数把单位圆盘映为上半平面, 反过来也一样. 这就证明了这两种几何学是相同的, 可以用这个函数把一个几何学的结果变为另一个几何学的结果.

和半平面模型一样, 当接近圆盘的边缘时, 双曲距离比欧几里得距离越来越大, 从双曲几何学的视角看来, 圆盘的直径是无穷大, 它实际上没有边缘. 图 2 表明, 可用一些全等图形把圆盘镶嵌铺装 (tessellation) 起来, 说这些图形全等是指其任意一个图形都可以用群中的一个变换变为任意另一个. 所以, 尽管这些图形看起来不都相同, 但是从双曲几何的视角看来, 它们却是大小相同形状也一样的. 圆盘模型中的直线或者是与单位圆周交成直角的 (欧几里得) 圆弧, 或者是经过圆盘中心的 (欧几里得) 直线线段.

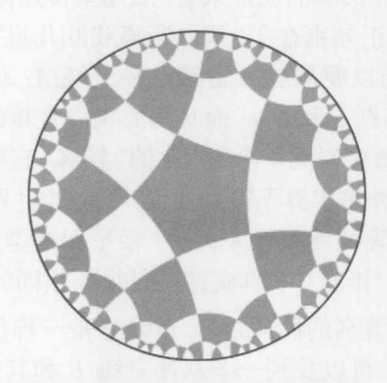


图 2 双曲圆盘的一个镶嵌铺装

双曲面模型可以解释这个几何学何以称为双曲几何学. 这一次, 点集合就是满足方程 $x^2+y^2=1+z^2,\quad z>0$ 的点 $(x,y,z)\in\mathbf{R}^3$ 的集合. 这是一个单叶旋转双曲面, 它是由平面 $z=0$ 上的双曲线 $x^2=1+z^2$ 绕 z 轴旋转生成的. $\mathrm{PSL}_2(\mathbf{R})$ 里的一般的变换, 就是这个单叶旋转双曲面上的某种"旋转", 而可以从真正的绕 z 轴

① 这件事是庞加莱本人在他写的《数学的创造》一文中讲到的. 这篇著名的文章有一个新的中文翻译, 可见《科学美国人》杂志的文集《现代世界中的数学》中译本 21 页, 这个译本由上海教育出版社于 2004 年出版.—— 中译本注

的旋转和 xz 平面上的 "双曲旋转" 合成, 所谓双曲旋转就是矩阵为

$$\begin{pmatrix} \cosh\theta & \sinh\theta \\ \sinh\theta & \cosh\theta \end{pmatrix}$$

的变换. 正如普通的旋转保持单位圆周一样, 双曲旋转保持双曲线 $x^2 = 1 + z^2$, 而让其内侧的点互相变动. 同样, 说这种变换会给出和上面同样的群, 这并非显然的事, 然而事实确实如此, 从而双曲模型和上面两个模型是等价的.

6.7 射影几何学

射影几何学被许多人看作是一门老旧的学科, 在中学里也不再教了, 但是它在现代数学中仍然起着重要作用. 我们在这里将集中注意于实射影平面, 但实际上, 任意维的具有任意标量的射影几何都是可能的. 这一点对于代数几何学家特别有用.

对射影平面有两种看法. 第一是这个点集合其实就是普通的平面再加上 "无穷远点". 变换群则由所谓的投影这种函数构成. 想要了解什么叫投影, 设想空间里有两个平面 P 与 P' 以及不在两平面中的任意一个平面上的点 x. 可以这样来把 P "投影" 到 P' 上. 若 a 是 P 上的一点, 它在这个投影下的像 $\phi(a)$ 就是 x 与 a 的连线与 P' 的交点 (如果这条直线平行于 P', 就说 $\phi(a)$ 是 P' 上的无穷远点). 这样, 如果在 x 处, 而在 P 上画了一幅画, 这幅画在投影 ϕ 下的像, 就是在 P' 上画出来的画, 这画看来就和 P 上那幅画一样. 然而, 这幅画事实上已经变形了, 所以投影 ϕ 已经对形状造成了差别. 要想把 ϕ 变为 P 本身的变换, 只要用一个刚性变换把 P' 移回到 P 就行了.

这样的投影显然不会保持距离, 然而它们确实保持着另外一些有趣的概念, 诸如点、直线、一种称为交比 (cross ratio) 的量, 最著名的还有圆锥截线. 圆锥截线就是平面截一个圆锥的交线, 它可以是一个圆、一个椭圆、一条抛物线, 或者一条双曲线. 从射影几何学的观点看来它们都是同一类的对象 (正如在仿射几何学里, 可以谈论椭圆, 但是谈不上圆作为椭圆的特例).

对射影平面的第二种观点是把它看作 $\mathbf{R}^3$ 中过原点的直线的集合. 因为一条这样的直线可由它与单位球面的两个交点决定, 所以也可以把这个集合看成就是单位球面, 但是与普通的球面有一个值得注意的区别, 就是把一条直径的两端 (称为互为 "对径点") 看成同一点 —— 因为它们相应于同一直线 (这件事很难想象, 但不是无法想象. 设想有这样一个 "世界", 不论在世界的一侧发生了什么事情, 那件事情的完全同样的复本 —— 这个世界的任何人、任何事, 都得有复本 —— 就会发生在这个世界另一侧的对应点 (即对径点) 处. 假设您已经在这个世界里过惯了, 而您从巴黎旅行到世界另一侧的巴黎的复本去, 那么, 您会以为巴黎的复本真是巴黎之

外的一个复本吗？城市看起来完全一样, 有完全同样的人, 而当您到达的时候, 您的复本也同时到达了 "真正的" 巴黎. 在这样的情况下, 说世界上只有一个巴黎, 只有一个您, 那就更加自然了. 只不过现在世界已经不再是球面的, 而是一个射影平面了.

在这样的观点下, 射影平面上的典型的变换可以这样得出来. 取任意的可逆线性映射并把它施加到 $\mathbf{R}^3$ 上. 这个映射把通过原点的直线仍然变成通过原点的直线, 所以可以看作是射影平面到其自身的函数. 如果一个可逆的线性映射是另一个的倍数, 它们在所有这种过原点的直线上效果相同, 所有这种变换的群就是稍加修改 $\mathrm{GL}_3(\mathbf{R})$, 而修改仅在于：任意两个矩阵若只相差一个非零的因子, 就应视为等价的. 这个群叫做射影特殊线性群 $\mathrm{PSL}_3(\mathbf{R})$, 它就是 $\mathrm{PSL}_2(\mathbf{R})$ 的 3 维等价物, 而 $\mathrm{PSL}_2(\mathbf{R})$ 我们已经见到过了. 因为 $\mathrm{PSL}_3(\mathbf{R})$ 大于 $\mathrm{PSL}_2(\mathbf{R})$, 所以射影平面就比双曲平面有更丰富的变换的集合, 这就是为什么得到保持的几何性质较少 (例如我们已经看到, 有一个有用的双曲距离的概念, 而没有明显的射影距离的概念).

6.8 洛仑兹几何学[①]

这是一个用于狭义相对论的几何学, 而以 4 维时空, 又称闵可夫斯基空间为模型. 它与 4 维的欧几里得几何学的主要区别在于它考虑的不是两点 (t,x,y,z) 和 (t',x',y',z') 的通常的距离, 而是以下的量

$$-(t-t')^2+(x-x')^2+(y-y')^2+(z-z')^2,$$

如果不是在 $(t-t')^2$ 前面的极为重要的负号, 它就是欧几里得距离的平方. 这反映了一个事实, 即时间和空间是极为不同的 (虽然它们交织在一起).

洛仑兹变换就是一个由 $\mathbf{R}^4$ 到 $\mathbf{R}^4$ 而且保持上面的 "广义距离" 不变的线性映射. 令 g 为映 (t,x,y,z) 到 $(-t,x,y,z)$ 的线性映射, 而 G 为 g 的相应的矩阵 (主对角线上的元素为 $-1,1,1,1$, 其余元素为 0 的矩阵), 我们可以抽象地定义洛仑兹变换为：矩阵 Λ 满足关系式 $\Lambda G\Lambda^{\mathrm{T}}=I$ 的线性映射, 这里 I 是 4×4 的单位矩阵, 而 Λ^{T} 表示 Λ 的转置矩阵 (一个矩阵 A 的转置就是由式子 $B_{ij}=A_{ji}$ 定义的矩阵 B).

对于一个点 (t,x,y,z), 如果 $-t^2+x^2+y^2+z^2>0$, 就说这个点是类空的; 而若 $-t^2+x^2+y^2+z^2<0$, 就说它是类时的; 而若 $-t^2+x^2+y^2+z^2=0$, 就说它位于光锥上. 所有这些都是真正的洛仑兹几何学的概念, 因为它们都是被洛仑兹变换所保持的.

洛仑兹几何学对于广义相对论也有基本的重要性, 广义相对论可以说就是对洛仑兹流形的研究. 这些都与黎曼流形密切相关, 将在 §6.10 中讨论. 关于广义相对论的讨论可见**广义相对论与爱因斯坦方程**[IV.13].

---

① 洛仑兹 (Hendrik Antoine Lorentz, 1853–1928), 荷兰物理学家, 爱因斯坦的狭义相对论的伟大先行者. —— 中译本注

6.9 流形与微分几何学

如果没有专门教过一个人, 他很自然地会以为地球是平坦的, 或者说它是一个平坦的曲面, 在曲面上面有房子、山等等. 然而现在我们知道了它其实更像球面, 看来像一个平面, 是因为它很大. 这方面有多种证据. 其一是, 如果站在海边的高岩上, 就会看到一条确定的地平线, 它并不太远但是它外边的船只都看不见了. 如果地球真是平坦的这就很难解释. 另一个证据是, 如果向着一个自以为是同一个方向一直向前走, 如果走得足够远, 就会又回到出发的地方. 第三个证据是, 如果沿着一条三角形路径旅行, 而三角形又足够大, 就会察觉出来, 它的三个角之和大于 180°.

相信最好的描述宇宙的几何学是 3 维欧几里得几何学, 或者说, 相信它是"正常的"几何学, 这是很自然的. 然而, 这是错误的, 和相信 2 维欧几里得几何学是地球表面最好的模型同样错误.

说真的, 考虑以洛仑兹几何学为时空的模型立刻就改善了这里的情况. 但是即令没有狭义相对论, 天文观测也不会给我们以任何特殊的理由, 认为宇宙是欧几里得几何学的最好的模型. 那么, 我们为什么会那么肯定, 很大的 4 维球体的 3 维表面不会给出更好的模型呢? 这有点像走了很长的距离, 就会把地球表面当作"正常的"平面一样, 说不定如果您坐着火箭飞上足够远而不改变航向, 最后也会回到原地.

数学上描述一个"正常的"空间是容易的. 只要对空间的一点按通常的方法给以坐标的三元组 (x,y,z) 就行了. 但是怎样来描述一个巨大的"球形"空间呢? 这要稍微难一点, 但也不太难, 可以对每一点给出四个坐标 (x,y,z,w), 但是加上一个条件, 即对于一个固定的 R, 它们要满足方程 $x^2+y^2+z^2+w^2=R^2$. 我们把这个 R 看成是宇宙的"半径", 这样就把 3 维空间描述为一个 4 维球体的表面, 正如方程 $x^2+y^2+z^2=R^2$ 是描述半径为 R 的 3 维球体的 2 维表面一样.

这个途径有一个反对意见, 就是它是依靠着一个很不可能的思想, 即宇宙是生活在一个更大的未曾观测到的 4 维空间里面. 但是, 可以回答这个反对意见. 我们刚才定义的对象, 即 3 维球面 S^3 也可以用所谓内蕴的方式来定义, 就是不需要参照任何包含的空间. 看出这一点的最容易的方法是先看 2 维球面, 然后再作类比.

所以, 让我们先想象一个行星, 上面是平静的水面. 如果在北极丢一块大石头到水里, 就有水波作为半径越来越大的圆传播开去 (在任意时刻, 这个圆都是一个纬圈). 然而到了一个适当的时刻, 这个纬圈达到了赤道, 在这以后, 它就会"收缩", 一直到最后, 波到达南极, 立刻成为能量的突然爆发.

现在假想在 3 维空间里突然发出光波 —— 例如可以是打开一盏明亮的灯. 现在波前不再是一个圆, 而是一个不断扩展的球面. 它可能扩展得很大很大, 然后又开始收缩, 但是不是收缩到原来的起点, 而是"从里翻到外地"收缩到另外一点. 从逻辑上说, 这是可能的 [只要注意 2 维情况的类比就可以看到这种可能性, 当上面

说的纬圈扩展到赤道以前, 北半球算是纬圈的内面, 而南半球算是外面; 但是一旦扩展越过赤道, 南半球就算是内面, 而北半球就 "从里翻到外地" 变成了外面]. 要可视地看到这种可能性, 当然要费点劲, 而且这个 "翻转" 的过程用不着求助于第四个维度. 更加切中要害的在于这样的讲法可以变成对于 3 维球面的一个数学上相容的真正 3 维的描述.

处理这个问题的一个不同的而且更加一般的途径是使用图册 (或图集, atlas). 一本世界地图集, 或称图册 (真正日常生活意义下的一本书的样子), 是由许多平面的地图页订成的 [例如有一页是美国地图, 另一页是加拿大地图. 这两页有互相重叠的部分, 因为这两个国家是挨在一起的. 因此对于重叠部分就需要说明, 这一页的某点, 对应于另一页的哪点, 例如多伦多, 在这两页地图上都可以找到, 但是在加拿大地图上, 它的位置就在图的南部, 而在美国地图上则在北部]. 虽然一个图册画的是 3 维宇宙中的一个对象, 但是地球表面的球面几何学却只需从平面的图页上读出. 这件事做起来虽然不太方便, 但确实是可能的, 例如可以这样来描述旋转: 第 17 页的某个部分要移动到第 24 页的某一部份, 虽然有点扭曲, 却是相似的.

这样做不仅是可能的, 而且一个 2 维曲面可以这样用 2 维图册来定义. 例如, 一个 2 维球面就可以用一个数学上干干净净的图册来定义如下: 这本图册仅有两页, 每一页都是一个圆形. 一页是北半球, 但是稍大一点, 越过赤道以便与南半球复叠起来; 另一页则是南半球, 但也稍大一点, 包含了北半球邻近赤道的一小块. 因为这两页地图都是平坦的平面, 就必定有点扭曲, 但是我们可以说得出扭曲有多大.

图册的概念很容易推广到 3 维情况. 现在, 每一 "页" 都是 3 维空间的一部分. 专业名词不说是 "(图) 页", 而说是 "区图"(chart): 一个 3 维图册就是若干 3 维区图的集合, 当然还需指明, 一个区图的某一部分如何对应于另一区图的哪一部分. 3 维球面有一个图册, 它推广了刚才讨论的 2 维球面的简单图册, 这个图册包含了两个立体的 3 维球体. 在一个球体靠近边缘 (球面) 的部分的点与另一球体靠近其边缘部分的点之间有一个对应, 这样就可以来描述其几何学了: 当您来到某个球体边缘附近时, 就会发现已经走到了重叠的区域, 同时走到了另一个球体里去了. 如果再往前走, 就一个球体而言, 您已经离开了它的地图, 但是第二个球体把您接过去了.

2 维和 3 维球面都是流形的基本例子, 其他在这一节见过的例子还有环面和射影平面. 非正式地说, 一个 d 维流形, 或简称为一 d 流形 M, 就是一个具有以下性质的几何对象: 它的每一点的某个邻域, 我们都感到像是 d 维欧几里得空间的一部分包围了这个点. 因为球面、环面、射影平面的很小一部分都非常接近于平面, 所以它们都是 2 流形, 虽然在 2 维情况下, 更常用 "曲面" 这个词以代替流形一词 (但是 "曲面" 并不一定是某个什么东西的 "表面", 记住这一点很重要). 类似地, 3 维球面就是一个 3 流形.

流形的正式定义使用了图册的概念. 说真的, 人们说: 图册就是一个流形. 这

是"是"这个字的典型的数学用法, 请勿与通常的用法混淆. 在实践上, 把流形想作区图的集合, 连带着还有区图各个部分如何互相对应的规则, 这种做法也不少见. 如果您想对流形作一般的推理, 而不是考虑特定的例子, 那么, 用图册和区图来定义它最为方便. 就本书的目的而言, 用我们开始时考虑 3 维球面的"外包"(extrinsic)方法来考虑 d 流形可能会更好, 就是把一个 d 流形看作一个生活在更高维空间里的 d 维"超曲面". 事实上, 有一个著名的纳什[①]定理指出, 所有的流形都是这样产生的. 但是要注意, 想找出一个简单的公式来定义这个超曲面并不总是易事. 例如, 2 维球面可以用简单的公式 $x^2+y^2+z^2=1$ 来描述, 而环面则要用一个稍微复杂而且有点人为痕迹的公式 $(r-2)^2+z^2=1$ 来描述, 这里的 r 就是 $\sqrt{x^2+y^2}$ 的简写. 要想找到两个洞的环面的公式就不容易了. 甚至是通常的环面, 也是像我们在 §3.3 中那样用商来描述要简单得多. 商也可以用来定义两个洞的环面 (见*福克斯群*[III.28]), 而我们深信所得的结果是一个流形, 其理由还在于每一点都有一个小邻域, 看起来就像欧几里得平面的一小部分. 一般说来, 任意一种构造方式, 只要是给出了一个"局部地像一个 d 维欧几里得空间"的对象, 就可以认为这个构造就是一个 d 流形.

流形的一个极为重要的特性在于对定义于其上的函数可以做微分[②]. 粗略地说, 设 M 是一个流形, f 是由 M 到 $\mathbf{R}$ 的函数, 要看 f 是否在 M 上一点 x 处可微, 首先要取 M 的一个包含 x 点的区图 (或区图的一个表示), 并认为 f 是定义在此区图上的函数. 因为区图是 d 维欧几里得空间 $\mathbf{R}^d$ 的一部分, 而我们可以在这样的集合上做微分, 所以可微性概念对于 f 也就有意义了. 当然, 要使这个定义在流形上也能用, 重要的是, 如果 f 属于两个重叠的区图, 则它应该对于这两个区图同为可微或不可微. 如果给出两个重叠区图的对应关系的函数 (称为转移函数) 本身就是可微的, 则同为可微或不可微就有了保证. 具有这个性质的流形就称为微分流形, 转移函数仅为连续而不一定可微的流形称为拓扑流形. 可以进行微分这件事使得微分流形的理论与拓扑流形理论大为不同.

上述思想很容易从实数值函数推广到从 M 到 $\mathbf{R}^d$ 的函数, 或者从 M 到另一流形 M' 的函数. 然而, 判定定义在一个流形上的函数是否可微, 比求它的导数要容易得多. 一个从 $\mathbf{R}^n$ 到 $\mathbf{R}^m$ 的函数在一点 x 处的导数是一个线性映射, 定义在一个流形上的函数也是一样. 然而这个线性映射的定义域并不是流形本身, 而是在所讨论的点 x 处的切空间.

关于这一点以及一般的流形, 更详细的讨论可见*微分拓扑*[IV.7].

---

①纳什 (John Forbes Nash, Jr.), 1928 年出生, 美国数学家, 因博弈论及其在经济学中的应用而获得 1994 年诺贝尔经济学奖. 在数学中, 他在微分拓扑学与偏微分方程上有重要的贡献.—— 中译本注

②原书用了 calculus 这个词, 似应包括积分. 但是流形上的积分是困难的问题, 例如可见*微分形式和积分*[III.16]. 同时, 正文中在此也只讲了微分, 所以这里译为"做微分".—— 中译本注

6.10　黎曼度量

设有球面上两点 P,Q, 怎样确定它们的距离? 答案依赖于如何定义球面. 如果定义它为所有使得 $x^2+y^2+z^2=1$ 的点 (x,y,z) 的集合, 那么 P,Q 就是 $\mathbf{R}^3$ 中的点. 所以可以用毕达哥拉斯定理算出它们的距离, 例如 $(1,0,0)$ 和 $(0,1,0)$ 的距离就是 $\sqrt{2}$.

然而, 我们真的想计算直线段 PQ 的长度吗? 这个直线段并不完全落在球面上, 所以用直线段来定义长度就与流形作为内蕴的有定义的对象这一思想完全不相容了. 幸而早前在讨论球面几何学时就知道有一个自然的定义可以避开这个问题: 可以定义 P,Q 之间的距离为连接这两点, 而且完全位于球面上的最短的路径的长度.

现在假设我们想要更一般地讨论流形上的点的距离. 如果流形是作为一个更大的空间的超曲面给予我们的, 就可以像在球面的情况那样定义此距离为最短路径的长度. 但是若流形是用别的方法给予我们的, 而我们仅仅知道的就是有一个方法可以证明每一点都包含在一个区图里面 —— 就是有一个邻域可与 d 维欧几里得空间的一部分联系起来 (为了讨论方便, 以后总设 d 为 2, 这对于我们的目的并无所失. 这样, 在此邻域与平面的一部分之间就有了对应关系). 这时, 定义距离的方法之一就是采用区图中的相应点的距离作为定义. 但是这样做, 至少引起了三个问题.

第一个问题是我们想要考虑的 P,Q 可能属于不同的区图. 然而这不是一个太大的问题, 因为我们真正想要计算的是路径的长度, 而只要能够定义充分接近的点之间的距离, 就可以算出路径之长, 而我们可以找出一个区图, 使得这两个充分接近的点都在其内.

第二个问题要严重多了, 那就是对于同一个流形有许多不同方法选择区图, 所以我们的想法并不一定引到流形的单个距离的概念. 更糟的是, 即令我们决定了一组区图, 它们还可能互相重叠, 当有重叠发生时, 无法使得各个区图里的距离相容.

第三个问题与第二个有联系. 球的表面是弯曲的, 而一个图册 (不论是数学意义下的还是日常生活意义下的) 里的区图是平坦的. 所以区图里的距离不可能精确地相应于球面本身的最短路径的长度.

从以上问题能得到的最重要的教训就是: 如果想在一个给定的流形上定义距离的概念, 怎样去做这件事, 总有多种选择. 非常粗略地说, 黎曼度量就是进行选择的方法.

一个不那么粗略的说法是: 一个度量意味着一个合理的距离概念 (准确的定义可以在 [III.56] 中找到). 一个黎曼度量就是决定无穷小距离的一种方法. 这些无穷小距离可以用来计算路径的长度, 而两点的距离就可以定义为它们之间的最短距

离. 为了看清怎样做这件事, 先考虑普通的欧几里得平面上路径的长度. 设 (x,y) 属于一条路径, 而 $(x+\delta x, y+\delta y)$ 是路径上另一点. 但非常接近于 (x,y) 点. 这时, 这两点间的距离是 $\sqrt{\delta x^2+\delta y^2}$. 要计算充分光滑的路径的长度, 就在此路径上取许多点, 而相邻两点都非常接近. 把它们之间的距离加起来, 就给出了一个很好的逼近. 取的点越多, 这个逼近就越好.

实际做的时候, 用微积分来算长度比较容易. 路径可以看成是一个动点 $(x(t), y(t))$ 在走, $t=0$ 时开始, $t=1$ 时停止. 如果 δt 很小, 则 $x(t+\delta t)$ 近似地就是 $x(t)+x'(t)\delta t$; $y(t+\delta t)$ 近似地则是 $y(t)+y'(t)\delta t$. 所以由毕达哥拉斯定理, $(x(t),y(t))$ 和 $(x(t+\delta t), y(t+\delta t))$ 的距离可以用 $\delta t\sqrt{x'(t)^2+y'(t)^2}$ 来逼近. 所以, 令 δt 趋向 0, 而把所有沿路径的无穷小距离积分起来, 就会得到路径长度的公式:

$$\int_0^1 \sqrt{x'(t)^2+y'(t)^2}\mathrm{d}t.$$

如果把 $x'(t), y'(t)$ 写成 $\mathrm{d}x/\mathrm{d}t, \mathrm{d}y/\mathrm{d}t$, 则可以把 $\sqrt{x'(y)^2+y'(t)^2}\mathrm{d}t$ 重写为 $\sqrt{\mathrm{d}x^2+\mathrm{d}y^2}$, 它是前面已经有了的 $\sqrt{\delta x^2+\delta y^2}$ 的无穷小版本. 这样, 就已经定义了一个通常写为 $\mathrm{d}x^2+\mathrm{d}y^2$ 的黎曼度量. 它可以看成是 (x,y) 和无限接近的点 $(x+\delta x, y+\delta y)$ 之间的距离的平方.

如果我们愿意, 可以证明两点 (x_0,y_0) 和 (x_1,y_1) 之间的最短路径是一直线, 从而最短距离是 $\sqrt{(x_1-x_0)^2+(y_1-y_0)^2}$(证明可见*变分方法*[III.94]), 然而, 刚才只是应用这个公式作为开始, 这个例子也还没有显示出黎曼度量真正的用处. 为了显示出它的作用, 我们要对讨论过的双曲几何学的圆盘模型再次给出更准确的定义. 在 §6.6 里说过, 当接近圆盘边缘时, 双曲距离比欧几里得距离就会越来越大. 一个更精确的说法就是: 单位圆盘就是满足条件 $x^2+y^2<1$ 的点 (x,y) 的集合, 而圆盘上的黎曼度量则由下面的表达式给出: $(\mathrm{d}x^2+\mathrm{d}y^2)/(1-x^2-y^2)$. 我们就是以这个式子来定义 (x,y) 和 $(x+\mathrm{d}x, y+\mathrm{d}y)$ 间的距离的平方的. 等价于此, 我们也说路径 $(x(t),y(t))$ 在这个黎曼度量下的长度是

$$\int_0^1 \sqrt{\frac{x'(t)^2+y'(t)^2}{1-x^2(t)-y^2(t)}}\mathrm{d}t.$$

更一般地说, 在平面的一部分上, 黎曼度量就是以下形式的表达式:

$$E(x,y)\mathrm{d}x^2+2F(x,y)\mathrm{d}x\mathrm{d}y+G(x,y)\mathrm{d}y^2,$$

我们就是要利用它来计算无穷小距离以及路径的长度 (在圆盘模型中, $E(x,y)$ 和 $G(x,y)$ 都是 $1/(1-x^2-y^2)$, 而 $F=0$). 使得这些距离均为正是很重要的, 而 $E(x,y)G(x,y)-F(x,y)^2>0$ 就能保证这件事. 我们当然也需要 E, F 和 G 满足一些光滑性条件.

这个定义可以直截了当地推广到高维情况. 在 n 维情况. 必须用以下形式的表达式:

$$\sum_{i,j=1}^{n} F_{ij}(x_1,\cdots,x_n)\mathrm{d}x_i\mathrm{d}x_j$$

来确定点 $(x_1,\cdots,x_n)$ 和点 $(x_1+\mathrm{d}x_1,\cdots,x_n+\mathrm{d}x_n)$ 的距离平方. 函数 $F_{ij}(x_1,\cdots,x_n)$ 形成一个 $n\times n$ 矩阵, 而我们要求它是一个正定矩阵, 即 $F_{ij}(x_1,\cdots,x_n)$ 必须等于 $F_{ji}(x_1,\cdots,x_n)$, 而上面那个确定距离平方的式子必须为正. 当然, 这些函数都应该是 $(x_1,\cdots,x_n)$ 的光滑函数.

最后, 我们既然已知道在欧几里得空间的一部分上面如何定义许多不同的黎曼度量, 就有了许多潜在的可能来在定义一个流形的区图上定义度量. 流形上的黎曼度量就是在各个区图上选择相容的黎曼度量的方法. 所谓 "相容" 就是指当两个区图重叠时, 在重叠的部分上距离一定要相同. 前面说过, 一旦做到了这一点, 就可以定义其上两点的距离为连接它们的最短路径的长度.

在一个流形上定义了黎曼度量以后, 就有可能来定义许多其他概念, 例如角度和体积. 还可以定义重要的曲率概念, 这个概念在条目里奇流[III.78] 中会讨论. 另一个重要的定义是测地线的定义, 它是欧几里得几何学里的直线概念在黎曼几何学里的类比. 所谓一条曲线 C 是测地线, 就是指若在其上任意给定两个相当接近的点, 曲线 C 的弧段总是给出它们之间的最短路径, 例如, 球面上的测地线.

从上面的讨论现在就应该清楚了, 在任意给定的流形上, 总有许多可能的黎曼度量. 黎曼几何学的一个重大主题, 就是从其中选择在某方面 "最好" 的黎曼度量. 例如, 如果在球面上选用那个显然的路径长度, 则得到的黎曼度量特别对称, 而这是一个很值得欢迎的性质. 特别是用了这一个度量后, 球面的曲率是处处相同的. 更一般地说, 要找出外加的条件附加在黎曼度量上. 理想的情况是这些条件要足够强, 使得只有这一个黎曼度量能够满足它, 至少是要使得满足这个条件的黎曼度量族会很小.

I.4　数学研究的一般目的

前一条目介绍了许多在整个数学中都会出现的概念, 这个条目则讨论数学家们对于这些概念做些什么事, 探讨哪一类的问题.

1. 解方程式

我们在前面几个条目里已经看到, 数学里面有许多对象和结构 (指数学类型的结构), 但是它们并不是放在那里等待我们去苦思冥想: 我们想对它们做些什么事. 例如, 给出了一个数, 我们会按照上下文去把它加倍、求平方或者求倒数; 给定了一

个适当的函数, 我们可能想去微分它; 给定了一个几何图形, 我们可能会想去作变换, 如此等等.

像这样的变化会给出无穷无尽的有趣的问题. 如果我们定义了一个数学程序, 那么去发明执行这个程序的技巧就是一个很显然的数学计划. 这就会引出关于这个程序的所谓的直接问题. 然而, 还有一类更深刻的所谓反问题, 其形式如下. 假设给出人们执行了什么样的程序, 得到了什么样的答案, 那么能不能搞清楚这个程序是作用在什么数学对象上的? 举一个例子, 假如我告诉您, 我拿了一个数, 把它平方, 结果是 9. 您能不能告诉我原来的数?

在这个情况, 答案或多或少是"能够": 它必须是 3, 除非负数也是许可的, 那时, -3 是另一个解.

如果我们想做更加形式的讨论, 就会说, 刚才是在研究方程 $x^2 = 9$, 而且发现它有两个解. 这样的例子提出了三个一再出现的问题.

- 一个方程是否有任何解?
- 如果有, 是否恰好有一个解?
- 这些解必在什么样的集合之内?

前两个问题称为解的存在与唯一性问题. 第三个问题在方程 $x^2 = 9$ 的情况下没有太大的意思, 但是在更复杂的情况下, 例如对于偏微分方程, 就可能是很细致而且重要的问题.

用更抽象的语言来说, 设 f 是一个*函数*[I.2 §2.2], 面前就是这样一个命题, 其形式是 $f(x) = y$, 直接问题就是给定了 x 求 y, 反问题则是给定了 y 求 x, 这个反问题就叫做解方程式 $f(x) = y$. 并不奇怪, 关于求解这种形式的方程式的问题与函数 f 的可逆性问题密切相关, 这个问题在 [I.2] 中有过讨论. 因为 x 和 y 可能是比数一般得多的对象, 解方程式的概念本身也就是非常一般的, 因此也就是数学的中心问题之一.

1.1 线性方程

小学生们最初遇见的方程典型地就是像 $2x + 3 = 17$ 这样的方程. 要解这样简单的方程, 我们把 x 看成未知数, 而未知数也得服从算术通常的法则. 利用这些法则, 就可以把这个方程化为简单得多的方程: 从方程双方减去 3, 就得到 $2x = 14$, 再用 2 除这个新方程的双方, 就得到 $x = 7$. 如果非常小心, 就会注意到, 我们实际上证明了: 如果有某个数 x, 使得 $2x + 3 = 17$, 那么这个数一定就是 7. 我们还没有证明的是: 确实有这样的数 x. 所以, 严格地说, 还应该有下一步, 即验证 $2 \times 7 + 3 = 17$. 现在, 它显然是对的, 但是对更加复杂的方程, 相应的论断就不一定总是对的, 所以最后这一步还是重要的.

方程 $2x + 3 = 17$ 称为线性方程. 这是因为加在 x 上的函数 (乘以 2, 然后再

加 3) 是一个线性函数. 正如刚才看到的, 只含一个未知数的线性方程是容易解的, 但是如果我们开始来处理多于一个未知数的方程, 情况就要微妙多了. 考虑含有两个未知数的方程的典型例子, 即方程 $3x+2y=14$. 这个方程有许多解, 选定一个 y 以后, 就可以置 $x=(14-2y)/3$, 于是就有了一对 (x,y) 满足这个方程. 要想使问题更难一点, 可以再加一个方程, 例如 $5x+3y=22$, 然后试着同时解出这两个方程. 这时的结果又是只有一个 (一组) 解 $x=2$ 以及 $y=4$. 典型情况下, 含两个未知数的两个线性方程恰好有一组解, 就如上面那两个方程那样. 如果从几何来看这个情况, 这是很容易理解的. 形如 $ax+by=c$ 的方程是 xy 平面上一条直线的方程. 两条直线正常地交于一个点, 例外情况是这两条直线相同, 这时它们交于无穷多个点, 或者它们平行, 这时它们根本不相交.

如果有好几个含有几个未知数的方程, 把它们看成含有一个未知的东西的一个方程, 在观念上会简单一些. 这听起来完全不可能, 但是, 如果允许这个未知的东西是一种更复杂的对象, 却是完全可能的. 例如 $3x+2y=14$ 和 $5x+3y=22$ 这两个方程可以写成单个含有矩阵和向量的方程

$$\begin{pmatrix} 3 & 2 \\ 5 & 3 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}=\begin{pmatrix} 14 \\ 22 \end{pmatrix}.$$

如果用 $\boldsymbol{A}$ 表示上面的矩阵, $\boldsymbol{x}$ 表示未知的向量, $\boldsymbol{b}$ 表示已知的向量, 则这个方程变为 $\boldsymbol{Ax}=\boldsymbol{b}$, 它看起来要简单多了, 尽管在事实上只是把复杂性隐藏在记号后面去了.

然而这个过程可不只是把垃圾扫到地毯下面藏起来, 而是还有更多的东西. 一方面, 简单的记号固然掩盖了这个问题的许多特定的细节, 另一方面却也把一些本来看不出来的东西揭示出来了, 现在有一个从 $\mathbf{R}^2$ 到 $\mathbf{R}^2$ 的线性映射, 想要知道的是哪一个向量 $\boldsymbol{x}$ 被映为向量 $\boldsymbol{b}$, 如果有这样的向量的话. 如果遇到的是一个特定的联立方程组的话, 这样重述问题并不造成大的区别 —— 我们需要做的计算还是一样的 —— 但是如果希望作一般的推理, 或者在新问题出现的地方遇到这些问题, 那么含有单个未知向量的矩阵方程就比含有几个未知数的联立的方程组要容易考虑得多. 这个现象会出现在整个数学中, 而且是研究高维空间的主要理由.

1.2 多项式方程

我们刚才讨论了线性方程从一个未知数到多个未知数的推广. 推广它们的另一个方向是把线性方程看成是 1 次多项式, 而考虑更高次数的函数. 例如在中学里, 我们就学习过怎样解诸如 $x^2-7x+12=0$ 这样的二次方程式. 更一般的多项式方程形如

$$a_nx^n+a_{n-1}x^{n-1}+\cdots+a_2x^2+a_1x+a_0=0.$$

解这样的方程, 就是求 x 的一个值 (最好是说求 x 的所有的值) 使得这个方程得以

满足. 这可能是一件说起来很显然的事, 但是在遇到简单如 $x^2-2=0$ 这样的方程, 或等价地, 即为 $x^2=2$ 这样的方程的时候, 就知道并不如此显然. 这个方程的解当然就是 $x=\pm\sqrt{2}$. 那么, 什么是 $\sqrt{2}$ 呢? 它的定义当然就是平方以后等于 2 的正数. 但是说 x 等于正的或负的且平方以后为 2 的数, 似乎还没有把 $x^2=2$ 这个方程 "解" 出来. 说 $x=1.4142135\cdots$ 也不完全令人满意, 因为这只是把一个没有尽头的式子写出了开头一小段, 而且也看不出来这个式子里有什么可以辨别出来的模式.

从这个例子可以得到两个教训. 其一是, 对于一个方程, 要紧的时常是解的存在与性质, 而不是是否能找到解的公式. 虽然当我们说方程 $x^2=2$ 的解是 $x=\pm\sqrt{2}$ 时, 并没有让我们学到什么, 但是这个论断中确实包含了一个并不全属显然的事实: 2 有平方根. 这一点通常是作为所谓中间值定理 (或本性类似的某个结果) 的推论而提出的. 这个定理指出, 若 f 是一个连续的实值函数, 而 $f(a)$ 和 $f(b)$ 各在零的一侧, 则在 a,b 之间的某处, 一定有一个实数 c 使得 $f(c)=0$. 这个结果可以用于函数 $f(x)=x^2-2$, 因为 $f(1)=-1$, 而 $f(2)=2$. 所以在 1, 2 之间一定有一个 x 使得 $x^2-2=0$, 亦即 $x^2=2$. 对于许多目的, 知道这个 x 的存在, 再加上知道定义这个 x 的性质使它为正且平方以后为 2, 这就足够了.

用类似的论证, 就知道所有的正实数都有正平方根. 但是当我们试图解更加复杂的二次方程时, 情况就不一样了. 这时有两条途径可供选择. 例如考虑方程 $x^2-6x+7=0$ 时, 我们会注意到, 当 $x=4$ 时, 它的值是 -1, 而当 $x=5$ 时, 其值是 2, 由此从中间值定理就知道, 这个方程在 4 与 5 之间有一个解. 但是如果用配方法, 就是把 x^2-6x+7 重写为 $(x-3)^2-2$, 就会得到两个解 $x=3\pm\sqrt{2}$. 从后一个方法我们学到的东西要比刚才更多. 用前面的方法我们已经证明了 $\sqrt{2}$ 的存在, 而且知道其值在 1 和 2 之间. 现在不仅是知道了方程 $x^2-6x+7=0$ 有一个解在 4 和 5 之间, 而且还知道了这个解与方程 $x^2=2$ 的解有密切的关系, 甚至可以说, 这个解正是从方程 $x^2=2$ 的解构造出来的. 这就证明了求解方程还有第二个重要的方面, 那就是在许多情况下, 解的显式的可解性是一个相对的概念. 只要给了方程 $x^2=2$ 的一个解, 在求解比较复杂的方程 $x^2-6x+7=0$ 时, 就不再需要从中间值定理得到什么新的输入, 需要的就仅仅是一点代数而已. 解 $x=3\pm\sqrt{2}$ 是由显式公式给出的, 但是这个表达式里的 $\sqrt{2}$ 就不是由一个显式公式来定义, 而是作为一个实数而定义的. 这个实数有一些性质, 而我们可以证明其存在.

解更高次的多项式方程比解二次方程要难得多, 而且由此产生了许多吸引人的问题. 特别是, 求解三次或四次方程有复杂的公式, 但是几百年来求解五次以及更高次的方程就一直是一个未解决的著名问题, 直到 19 世纪, 阿贝尔[VI.33] 和伽罗瓦[VI.41] 才证明了显式解的公式是找不到的. 关于这些问题, 详见五次方程的不可解性[V.21], 另一篇有关多项式方程的条目是代数的基本定理[V.13].

1.3 多变元的多项式方程

设有这样的方程

$$x^3+y^3+z^3=3x^2y+3y^2z+6xyz,$$

我们可以直接看出来它有许多解: 如果固定 x 和 y, 就得到一个 z 的三次多项式方程, 所有的三次多项式方程都有 (至少一个) 实解, 所以对于每一个固定的 x 和 y, 都有某个 z 使得三元组 (x,y,z) 成为这个方程的解.

因为三次方程解的公式十分复杂, 准确地描述所有这些三元组 (x,y,z) 的集合就没有什么可以启发人的地方了. 但是, 若把解的这个集合看成一个几何对象 —— 准确地说是空间里的一个 2 维曲面 —— 并且考虑一些关于它的定性的问题, 就可以从中学到不少东西. 例如我们可能希望了解其大体的性质如何, 用拓扑学[I.3 §6.4] 的语言, 可以把这些问题说清楚.

当然还可以进一步推广来考虑几个多项式方程的同时求解. 理解这些方程组的解集合属于代数几何[IV.4] 的领域.

1.4 丢番图方程

前面提到过, 一个特定的方程是否有解, 需视允许在何处求解而异. 如果只允许 x 为实数, 则方程 $x^2+3=0$ 就没有解, 但是在复数里, 它就有两个解 $x=\pm\mathrm{i}\sqrt{3}$. 方程 $x^2+y^2=11$ 有无穷多个解, 但是如果求的是实的 x 和 y, 而且要求 x 和 y 都是整数, 这个方程就没有解.

上面的例子是典型的丢番图方程, 凡见到这个名词就表示要求它的整数解. 最著名的丢番图方程就是费马方程 $x^n+y^n=z^n$. 感谢怀尔斯 (Andrew Wiles) 的工作, 现在已经知道当 n 大于 2 时, 它没有正整数解 (见费马大定理[V.10], 与此形成对照, 方程 $x^2+y^2=z^2$ 却有无穷多个 [整数] 解). 现代的代数数理论[IV.1] 的很大一部分都是在直接或者间接地讨论丢番图方程. 正如对于实数或复数的方程一样, 讨论丢番图方程解的集合的结构是富有成果的, 这类研究属于算术几何[IV.5] 的领域.

丢番图方程的一个值得注意的特点是它们极为困难. 所以自然地会怀疑, 对于它们是否可能有一个系统的处理方法, 这是希尔伯特[VI.63] 在 1900 年提出的著名问题清单中的第 10 个问题. 但是一直到 1970 年 Yuri Matiyasevich 才在 Martin Davis, Julia Robinson 和 Hilary Putnam 的工作基础上指出, 这个问题的回答是否定的 (这一点在条目停机问题的不可解性[V.20] 里有进一步的讨论).

这个问题的解决, 重要的一步是在 1936 年由丘奇[VI.89] 和图灵[VI.94] 做出的. 只是通过 (以两种不同方法) 把算法概念形式化 (见算法[II.4§3] 和计算复杂性[IV.20]), 从而把 "系统的处理" 这个概念弄清楚以后, 才走出了这一步. 在计算机

时代以前, 这是不容易的, 但是我们现在却可以把希尔伯特第 10 问题的解决重述如下: 想找一个计算机程序使得在输入任意的丢番图方程后, 如果这个方程有解, 它就一定会输出 "YES", 无解的时候就一定会输出 "NO", 而且从不出错, 这是做不到的.

关于丢番图方程, 这告诉了我们什么呢? 我们再也不能梦想会有一个囊括所有这种方程的最终的理论, 相反, 我们被迫集中注意于这种方程的特殊的类别, 并且对它们发展不同的解法. 如果不是因为丢番图方程与数学的其他部分的很一般的方程有值得注意的联系, 这似乎会使得在解决了最初几个方程以后, 丢番图方程就没有趣味了. 例如方程 $y^2 = f(x)$(其中 $f(x)$ 是一个三次多项式) 看起来很特殊, 事实上, 它所定义的椭圆曲线[III.21] 却是现代数论 (包括费马大定理的证明) 的中心问题. 当然费马大定理本身也是一个丢番图方程, 但它的研究又导致了数论的其他部分的重大发展. 应该得出的正确的结论可能是: 解一个特殊的丢番图方程, 如果其结果不只是在已经解决的方程的单子上添加一个 (可惜, 事实时常就是这样的) 而已, 那么, 它是吸引人的, 是值得去研究的.

1.5 微分方程

迄今为止, 我们考虑的方程都是以数或 n 维空间的一点 (即一串 n 个数) 为未知的东西的. 要生成这样的方程, 我们作算术的基本运算的不同组合, 然后把它们施加到未知的东西上去.

下面给出两个著名的微分方程以便与过去讨论过的方程作比较:

$$\frac{\mathrm{d}^2x}{\mathrm{d}t^2} + k^2x = 0,$$
$$\frac{\partial T}{\partial t} = \kappa\left(\frac{\partial^2 T}{\partial x^2} + \frac{\partial^2 T}{\partial y^2} + \frac{\partial^2 T}{\partial z^2}\right).$$

第一个是 "常" 微分方程, 是简谐运动方程, 它有通解 $x(t) = A\sin kt + B\cos kt$; 第二个是 "偏" 微分方程, 是热方程, 在一些基本的数学定义[I.3§5.4] 里讨论过它.

有许多理由说明求解微分方程在精巧性上是一个飞跃. 一个理由在于, 现在未知的东西是函数, 它比起数或者 n 维空间的点来是复杂得多的对象 (例如, 上面的第一个方程要求 t 的函数 x 在微分两次以后, 还原为原来的函数, 但乘上因子 $-k^2$). 第二个理由是, 现在施加于函数上的运算微分和积分, 它们远不如加法和乘法那么 "基本". 第三个理由是, 微分方程, 哪怕是很自然很重要的方程, 可以用 "封闭形式" 解出的, 就是用一个公式来表示未知函数 f 的, 只是例外而非常规.

现在回到第一个方程. 对于函数 f, 如果用 $\phi(f)$ 来表示对于 f 的一个函数 (变换)$(\mathrm{d}^2f/\mathrm{d}t^2 + k^2f)$, 则这个变换是一个线性映射, 意思就是由 $\phi(f+g) = \phi(f)+\phi(g)$ 以及对任意常数 a 有 $\phi(af) = a\phi(f)$. 这意味着微分方程可以看成是一个矩阵方程

推广到无穷多维的情况. 热方程也有同样的性质: 如果定义 $\psi(T)$ 为

$$\frac{\partial T}{\partial t}-\kappa\left(\frac{\partial^2 T}{\partial x^2}+\frac{\partial^2 T}{\partial y^2}+\frac{\partial^2 T}{\partial z^2}\right),$$

则 ψ 是另一个线性映射. 这种微分方程称为线性的, 它们与线性代数明显的联系使得它们容易求解得多 (这方面一个有用的工具是傅里叶变换[III.27]).

那些更加典型的方程, 即不能用封闭形式解出的方程又如何? 那时, 焦点就又一次转移到是否有解存在? 如果有, 它们又有哪些性质? 和多项式方程一样, 这要依赖于把什么当成是可以允许的解. 有时, 我们就像又处在研究方程 $x^2=2$ 时的境地: 证明解的存在并不难, 只需要给它取一个名字就行了. 方程 $\mathrm{d}y/\mathrm{d}x=\mathrm{e}^{-x^2}$ 就是一个简单的例子. 在某种意义下, 它是不能解出来的, 可以证明, 找不到一个由多项式、指数函数[III.25]、三角函数[III.92] 等等 "基本的" 函数构建出来而微分以后又会给出 e^{-x^2} 的函数. 然而在另一种意义下, 这个方程又很容易求解 —— 只需要把函数 e^{-x^2} 积分一下就行了, 所得到的函数 (除以 $\sqrt{2\pi}$ 以后) 就是正态分布[III.71§5] 函数. 这个函数在概率论里面有基本的重要性, 所以就给了它一个名字 (记号)Φ.

在绝大多数情况下, 写出解的公式是没有希望的事情, 哪怕是把积分一个 "已知" 函数也算是求出了解也一样. 一个著名的例子是三体问题[V.33]: 给出空间里的三个运动的物体 (质点), 并设它们以引力互相吸引, 问它们会怎样继续运动? 用牛顿定律可以写出描述这一情况的微分方程. 对于两个运动着的物体, 牛顿[VI.14] 解出了相应的方程, 并由此解释了为什么行星绕太阳沿椭圆轨道运动, 但是对于三个或更多的物体, 这些微分方程证明是非常难解的. 现在已经知道了, 这种难解的情况有很深刻的理由: 这时, 这些微分方程会导致混沌性态 (关于混沌, 较详细的讨论可以参看动力学[IV.14]). 然而, 这就打开了研究混沌和稳定性这些非常有趣的问题的大道.

有时候, 有方法证明解是存在的, 哪怕这些解不能容易地确定下来. 这时, 可以不要求得到精确的公式, 而只希望得到一般的描写. 例如, 如果这个方程有着时间依赖性 (例如热方程和波方程就都有), 人们就会问, 解是否随时间而衰减、爆破, 或者大体上不变? 这些更加定性的问题称为渐近性态问题, 有一些技巧来回答这一类的某些问题, 尽管没有干净利落的公式把解给出来.

和丢番图方程的情况一样, 偏微分方程包括非线性偏微分方程中有一些特殊而又重要的类, 可以把解准确地写出来. 这就给出了一种非常不同的研究风格: 人们又一次关注于解的性质, 但是这一次是本性上更加代数化的性质, 就是说, 解的公式将要起更重要的作用, 见线性与非线性波以及孤子[III.49].

2. 分类

如果一个人想理解一个数学结构, 例如群[I.3 §2.1] 或者一个流形[I.3 §6.9], 他

要做的第一件事就是找到足够多的例子, 有时候例子是很容易找的. 这时, 例子就会多到令人迷惑的一大堆, 但又理不出头绪来. 然而, 时常是这些例子必须要满足的条件相当严格, 这时, 可能得到的例子会成为一个无限长的单子, 使得各个具体例子都包括在这个单子里面. 例如, 可以证明域 $\mathbf{F}$ 上的任意的 n 维向量空间[I.3 §2.3] 都同构于 $\mathbf{F}^n$, 这意味着只要有一个正整数 n 就足以完全决定这个向量空间. 这时, 例子的清单就是 $\{0\}, \mathbf{F}, \mathbf{F}^2, \mathbf{F}^3, \mathbf{F}^4, \cdots$, 这时, 就说得到了相关的数学结构的一个分类.

分类是非常有用的, 因为如果能对一个数学结构进行分类, 就有了一个新方法来证明关于这个结构的结果, 而不必从这个结构所必须满足的公理来导出它们, 而只需要检验这个结果是否对于这个单子里的每一个例子都成立, 如果是, 我们就深信已经一般性地证明了这个结果. 这样做并不总是比更加抽象的公理方法更容易, 但是有时候确实要容易一些. 说真的, 有一些结果就是用分类来证明的, 而至今还不知道怎样用别的方法证明. 更一般地说, 对于一个数学结构, 知道的例子越多, 就越容易思考这个结构 —— 检验假设、寻找反例等等. 如果已经知道了一个结构所有的例子, 则对于某些目的, 就已经完全懂得了这个结构.

2.1 *确定建造的砖石以及族*

有两种情况典型地导致有趣的分类定理, 这两种情况的界限有时不甚清晰, 但是区别仍然足够明显, 而值得去加以区别, 所以在这一小节和下一小节分别讨论这两种情况.

作为第一种情况的例子, 考虑一种称为正多胞体 (polytope) 的数学对象. 多边形、多面体, 以及它们的高维推广都是多胞体. 正多边形就是那些所有各边长度都相等且所有顶角也都相等的多边形; 正多面体就是那些各个面都是全等的正多边形而在每个顶点上又都有相同个数的棱在那里相遇的多面体. 更一般地说, 一个高维多胞体为正, 就是说它有尽可能多的对称性, 虽然精确的定义还有点难 (在三维情况下, 现在有一个正多面体的新定义, 它等价于上面所给的定义, 但是又比较容易推广: 我们说一个旗 (flag) 就是一个三元组 (v, e, f), 其中 v 是多面体的一个顶点, e 是通过这个 v 的棱, 而 f 是一个以 e 为边的面. 说一个多面体是正多面体, 就是说对于任意两个旗 (v, e, f) 和 (v', e', f') 都有多面体的一个对称, 变 v 为 v', 变 e 为 e', 变 f 为 f').

很容易看到正多边形是 2 维的, 对每一个正整数 $k > 2$, 都可以找到一个正 k 边形. 在 3 维情况, 正多面体就是著名的柏拉图多面体, 它们是正四面体、立方体 (即正六面体)、正八面体、正十二面体和正二十面体. 证明只有这五种正多面体也不算太难, 因为在每一个顶点处至少有 3 个面相遇, 而以此顶点为顶的角之和必然小于 $360°$. 这些限制表明, 过一个顶点的面可以有 3 个、4 个或 5 个正三角形, 或

者 3 个正方形, 或者 3 个正五边形. 它们就依次分别给出正四面体、正八面体、正二十面体、立方体和正十二面体.

[现在我们想在更高维的空间里找到正多边形和正多面体的类比. 刚才定义的正多边形和正多面体中, 只有一部分这样的类比很清楚]. 先看正三角形和正四面体. 在 $\mathbf{R}^n$ 中取 $n+1$ 个点, 使其中任意两点的距离均为 1, 它们就构成一个正单形 (regular simplex) 的顶点, 这个正单形就是 2 维的正三角形与 3 维的正四面体的推广. 再看 $\mathbf{R}^n$ 中适合条件 $0 \leqslant x_i \leqslant 1, i=1,2,\cdots,n$ 的点 $(x_1,x_2,\cdots,x_n)$ 的集合, 它自然是立方体在高维情况下的类比. 最后看 $\mathbf{R}^n$ 中适合条件 $|x_1|+|x_2|+\cdots+|x_n| \leqslant 1$ 的点 $(x_1,x_2,\cdots,x_n)$ 的集合, 就是正八面体在 $\mathbf{R}^n$ 中的类比, 因为 3 维的正八面体是适合条件 $|x|+|y|+|z| \leqslant 1$ 的点 $(x,y,z) \in \mathbf{R}^3$ 的集合. [总之, 由正四面体、正六面体和正八面体都可以给出可称为正多胞体的一个无穷序列].

除此而外, 正十二面体和正二十面体会不会各自也导出多胞体的无穷序列, 并可以把它们称为正多胞体? 这一点并不显而易见, 而结果是它们不会. 事实上, 除了在 4 维情况下还可以再找到三个例子以外, 再也没有其他可以称为正多胞体的例子了. 而这三个无穷序列, 再加上这三个例子就构成了正多胞体的完全的清单, 这三个例子很值得注意, 其中一个具有 120 个 “3 维面”, 各是一个正十二面体, 它有一个 “对偶”①, 以 600 个正四面体为其 3 维 “面”. 第三个例子则可用坐标来介绍: 它有 16 个顶点, 坐标为 $(\pm1,\pm1,\pm1,\pm1)$, 还有 8 个坐标为: $(\pm2,0,0,0),(0,\pm2,0,0),(0,0,\pm2,0),(0,0,0,\pm2)$.

以上就是所有的正多胞体, 这一个类比上面简述的 3 维情况下的结果要难证明得多. 这个完全的清单是由 Schläfli 在 19 世纪中叶得出的; Donald Coxeter 在 1969 年证明了, 再没有其他例外了.

所以, 在 3 维和更高维情况下, 正多胞体分成三个序列 —— 就是 n 维的正四面体序列、正六面体序列、正八面体序列 —— 再加上五个 “例外的” 例子, 即 3 维的正十二面体和正二十面体, 还有刚才描述的三个 4 维多胞体的例子. 在许多分类定理中, 这个情况是一个典型. 这些例外的例子时常称为 “散在” 的 (sporadic) 例子, 时常有非常高的对称性 —— 使我们几乎不敢期望这样高的对称性居然是可能的, 如果可能也只是偶然会有的好运气. 在不同的分类定理的结果中的这些序列和散在的例子时常互有紧密的联系, 这是那些看起来毫无关系的领域互相有深刻的联系的一个信号.

有时, 我们并不打算把所有的某一类数学结构加以分类, 而是从中识别出某些 “基本的” 结构, 使得其他的结构全可以由它们简单地构造出来. 素数的集合就是一个好的类比: 所有的整数都可以由它们以积的方式构造出来. 又如, 所有的有限群

① 柏拉图正多面体各有一个对偶: 正六面体和正八面体互为对偶; 正十二面体和正二十面体互为对偶; 正四面体自己与自己对偶. 对于正多胞体, 对偶的概念也是有用的. 详见对偶[III.19 §1].—— 中译本注

都是一些称为“单群”的基本的群的“乘积”. 有限单群的分类[V.7], 20 世纪数学最著名的定理之一, 将在第 V 部分讨论.

关于这种类型的分类定理, 也可见李的理论[III.48].

2.2 等价性, 不等价性, 以及不变式

在数学中有许多这样的情况, 两个对象严格地说是不相同的, 但是我们对它们的差异并不关心. 在这样的情况下, 我们认为这两个对象“本质上相同”或“等价”. 这种等价是用等价关系[I.2 §2.3] 来形式地表示的.

例如, 如果两个图形中, 有一个图形可以连续地变为另一个, 拓扑学家就认为这两个图形本质上是一样的, 这一点我们已经在 [I.3 §6.4] 中见到过. 在那里已经指出, 一个球面在这个意义下与一个立方体 (表面) 是同样的; 我们也能看到, 轮胎表面, 即环面, 和一个茶杯的表面本质上是一样的. [说到茶杯表面, 是说把茶杯的杯体连同它的柄看成“中空”的, 然后好像吹气球似地把茶杯吹胀起来, 再让它的柄的部分胀起来, 而把杯体部分捏缩下去, 这样茶杯就连续变形成一个轮胎形状的曲面了]. 直观地说, 非常明显, 球面和环面本质上是不一样的, 但是这一点证明起来就难多了.

为什么不等价比等价要难证明呢? 答案在于, 要证明两个对象等价, 只要找到一个变换就可以证明等价性, 而要证明两个对象不等价, 就要考虑一切可能的变换, 并且证明没有一个管用. 我们怎么能够排除会有一个极为复杂的没法看得见的连续变换, 偏会非常引人注目地把一个球面变成一个环面呢?

下面是证明的要点. 球面和环面都是紧的可定向曲面的例子, 这句话粗略的意思就是, 它们都是 2 维的图形, 占据空间的一个有限的部分, 而且没有边缘. 给定了这样一个曲面, 就可以找到一个由三角形拼接起来而且拓扑上与这个曲面相同的等价的曲面. 欧拉[VI.19] 有一个著名的定理, 指出:

令 P 为一个拓扑上与球面相同的多面体, 并设它有 V 个顶点、E 条棱以及 F 面, 则 $V-E+F=2$.

例如, 设 P 为一个二十面体, 则它有 12 个顶点、30 条棱以及 20 个面, 这时 $12=30+20=2$.

对于这个定理, 三角形是平坦的这一点并不重要: 我们可以把这些三角形画在原来的球面上, 当然这样一来这些三角形都成了球面三角形. 但是这样画了以后数它的顶点、棱和面还是一样容易, 定理也仍然成立. 画在球面上的这个三角形网格称为球面的三角剖分.

欧拉定理指出, 不管对球面作什么样的三角剖分, 总有 $V-E+F=2$. 此外, 如果我们作了三角剖分的曲面并非球面, 而是一个拓扑上与球面等价的另一个曲面, 这个公式也是对的, 因为三角剖分可以连续形变而 V,E,F 不会改变.

更一般地说, 我们可以对任意曲面作三角剖分, 然后估算 $V-E+F$, 结果称为这个曲面的欧拉示性数. 为使这个定义有意义, 需要下面的事实, 它是欧拉定理的推广 (其证明也不比原来的结果更难).

(i) *虽然曲面可以用多种方法作三角剖分, 量 $V-E+F$ 对所有的三角剖分都一样.*

如果对曲面作连续变形, 同时也对三角剖分作连续变形, 就可以得出新曲面和老曲面的欧拉示性数一样. 换句话说, 事实 (i) 有下面有趣的推论:

(ii) *如果两个曲面互为连续形变, 则它们有相同的欧拉示性数.*

这一点给出了证明曲面不等价的潜在可能的方法: 如果它们有不同的欧拉示性数, 它们就不会互为连续形变. 环面的欧拉示性数为 0(可以任作一个三角剖分, 然后就能算出它的 $V-E+F$), [因为这个结果与球面的欧拉示性数为 2 不一样, 所以就知道球面和环面不会等价].

欧拉示性数是所谓不变式的一个例子. 不变式就是一个函数 Φ, 其域是我们所研究的那一类全部对象的集合, 而且具有如下的性质: 如果两个对象 X 和 Y 等价, 则 $\Phi(X)=\Phi(Y)$. 为了证明 X 和 Y 不等价, 只需找到一个不变式 Φ 使得 $\Phi(X),\Phi(Y)$ 不相等即可. 有时 Φ 是一个数 (欧拉示性数就是这样), 但它们时常也可以是更复杂的数学结构, 例如多项式或群.

完全有可能 $\Phi(X)=\Phi(Y)$, 但是 X 和 Y 并不等价. 一个极端的例子是, 对于一切对象 X 都恒等于零的 Φ, 它当然也是一个不变式. 然而, 有时证明对象不等价是如此困难, 以至于不变式尽管只能部分时间有用, 也认为不变式是有用而且有趣的.

对于一个不变式 Φ, 我们时常寻求它的两种主要性质, 而这两种性质又时常是向两个相反方向起作用的. 其一是要它尽可能的细, 意思是, 只要 X 和 Y 不等价, $\Phi(X)$ 就和 $\Phi(Y)$ 不同. 其二是要能够实际地确定何时 $\Phi(X)$ 就是和 $\Phi(Y)$ 不同. 一个不变式哪怕是很细, 如果无法算出来, 那就没有大用处 (一个极端的例子是 "平凡的" 不变式, 即映一个对象入自己的等价类这样的不变式. 它确实细到了极点 [如果 X 和 Y 不等价, 它们当然不在同一个等价类中, 因此 $\Phi(X)$ 自然和 $\Phi(Y)$ 不同], 但是除非有独立的方法确定这个不变式, [即找出这个对象的等价类], 那么它对于原来提出的证明两个对象不等价这个问题, 并不是一个进展). 所以, 最强有力的不变式大概会是那些既能够计算出来, 又不太容易计算出来的不变式.

在紧的可定向曲面的情况下, 我们是运气很好的: 欧拉示性数不仅是容易计算的不变式, 又确实能把所有的紧的可定向曲面作完全的分类. 说准确一点, 一个数 k 是欧拉示性数, 当且仅当存在一个非负整数 g 使得 $k=2-2g$(所以可能的欧拉示性数只能是 $2,0,-2,-4,\cdots$, [相应于 $g=0,1,2,\cdots$]. 具有相同欧拉示性数的紧的可定向曲面必是等价的, 而数 g 就完全地确定了这个曲面. 它称为曲面的亏格, 而可以几何地解释为曲面所具有的 "洞" 的个数 (所以球面的亏格为 0, 环面的亏格为 1).

关于不变式的其他例子, 请看代数拓扑[IV.6] 和纽结多项式[III.44].

3. 推广

当一个重要的数学定义已经提出, 一个重要的数学定理已经证明, 事情就此了结是罕有的情况. 然而, 不论一项数学工作如何清晰, 总还有更好了解它的余地, 这样做最常用的方法之一, 就是把它陈述为一个更广泛的东西的特例. 有不同种类的推广, 这里只讨论其中的几个.

3.1 弱化假设和强化结论

1729 这个数很有名①, 因为它可以用两种不同方式写成两个 [正整数的] 完全立方的和, 就是 1^3+12^3 和 9^3+10^3. [而且是这类数中最小的一个]. 让我们试着来决定, 是否有一个数可以用四种不同方式写成四个完全立方之和.

初看起来, 这个问题似乎是难得令人吃惊, 如果真有这样的数, 这个数必定是很大很大, 如果想一个数接着一个数地去试, 又必定是极为冗长乏味. 那么, 可不可以做得更好一些呢?

回答是必须把假设弱化. 我们想解决的问题属于下面的一般类型. 给出一个正整数序列 $a_1,a_2,a_3,\cdots$, 而且告诉了我们这个序列具有某个性质. 然后要证明, 一定存在一个正整数, 使得它可以用十种不同的方式写成这个序列中四项之和. 这样思考问题可能有一点人为造作的味儿, 因为假设了这个序列是 "完全立方数的序列", 因为这个性质的序列 [比起所谓 "具有某个性质" 的序列] 显得过于特殊, 所以比较自然的想法是把这个问题看成是一个 [特定] 序列的鉴别问题. 然而, 这种思考问题的方式鼓励我们考虑有这样的可能性, 就是这个结论可能对于广泛得多的序列仍然为真, 而结果确实如此.

有 1 000 个完全立方数小于或等于 1 000 000 000, [因为 1 000 000 000 就是 $1\ 000^3$]. 我们将会看到正是这件事, 就足以保证 "存在一个整数, 而它可以用十种不同方式写成四个完全立方数之和". 具体说来, 我们的问题变成证明: 若 $a_1,a_2,a_3,\cdots,a_{1000}$ 是任意的正整数序列, 而且其各项均不大于 1 000 000 000, 则必存在一个正整数, 可以用十种不同方式写为此序列的四项之和.

为了证明这件事, 我们先要注意到, 从序列 $a_1,a_2,\cdots,a_{1000}$ 中任意取四项的方式有 $1\ 000\times999\times998\times997/24$ 种, 这个数小于 $40\times1\ 000\ 000\ 000$(即 400 亿), 而这个序列中任意四项之和必不大于 $4\times1\ 000\ 000\ 000$(即 40 亿), [所以现在有 400 亿个

① 说这个数很有名是因为据说有一次哈代到医院看望拉玛努金时说, 他今天乘坐的出租车车号是 1729. 哈代问拉玛努金这个数有什么特别? 拉玛努金几乎是不假思索就告诉哈代, 它可以用两种不同的方式, 写成两个完全立方数的和. 因为这个故事广为流传, 所以 1729 有时被称为哈代–拉玛努金数. 我在正文中对于完全立方加进了 "正整数" 的限制, 这是很重要的, 因为哈代说过 1729 是最小的具有这种性质的数. 如果也允许负整数, 那么最小的具有这种性质的数是 $91=6^3+(-5)^3=4^3+3^3$.—— 中译本注

不大于 40 亿的数, 其中必有重复的数], 平均说来, 取相同值的数应该有十个以上. 所以, 在 "400 亿个数" 中, 至少有一个会取 "40 亿个值" 的某一个十次以上. 证毕.

为什么用这种方式把问题推广会有助于问题的解决? 人们可能会以为, 在证明一个结果时, 假设越少, 证明就越难. 然而时常并不如此. 假设越少, 在用这个假设来证明时, 需要作的选择也越少, 这有时会加快对于证明的搜寻. 如果没有把这个问题推广如上, 就会有过多的选择. 例如, 可能会试着去解非常困难的含立方项的丢番图方程, 而不是像现在这样, [只是在比较选取四项的方式的数目, 与序列中任意四项之和的大小] 时作简单的计数问题.

我们也可以认为上面的推广就是结论的强化：原来的问题只是一个关于立方的命题, 而我们的证明则多得多. 弱化假设与强化结论, 并没有清晰的区别, 因为如果要求证明一个命题 $P \Rightarrow Q$, 就总可以把它重述为证明 $\neg Q \Rightarrow \neg P$, 因此, 如果弱化 P, 就可以说是弱化了 $P \Rightarrow Q$ 的假设, 也可以说是强化了 $\neg Q \Rightarrow \neg P$ 的结论.

3.2 证明一个更抽象的结果

模算术[III.58]里有一个著名的结果, 称为费马小定理：如果 p 是一个素数, 而[正整数]a 不是 p 的倍数, 则 a^{p-1} 除以 p 时, 余数必为 1. 就是说 $a^{p-1} \bmod p$ 必定同余于 1.

这个结果有几种证明, 其中之一是谋求推广的好例证. 以下就是其论证的概要. 第一步, 证明数 $1, 2, \cdots, p-1$ 在 $\bmod p$ 的乘法下构成一个群[I.3 §2.1]($\bmod p$ 的乘法就是说相乘以后要除以 p 并取其余数. 举例来说, 若取 $p = 7$, 则 3 与 6 的积 "mod7" 是 4, 因为 4 是 $3 \times 6 = 18$ 除以 7 所得的余数). 第二步, 注意到, 若 $1 \leqslant a \leqslant p-1$, 则 a 的幂 mod$p$ 构成此群的子群, 而且这个子群的大小是最小的使得 $a^m \equiv 1, \text{mod} p$ 的整数 m, 然后应用拉格朗日定理, 即群的大小必定可用子群的大小整除. 现在群的大小是 $p-1$, 所以 $p-1$ 可用 m 整除, 但是 $a^m \equiv 1, \text{mod} p$, 所以 $a^{p-1} \equiv 1, \text{mod} p$. 定理证毕.

这个论证表明, 如果恰当地看待, 费马小定理只是拉格朗日定理的一个特例 (不过, 这里的 "只" 字却难免会产生误导, 因为按照这里所说, 整数 mod$p$ 成为一个群并不是完全显然的. 这个事实可以用欧几里得算法[III.22] 来证明).

费马本人不可能这样来看他的定理, 因为在他证明这个定理时, 群的概念还没有发明. 所以, 群的抽象概念帮助人们以全新的方式来看待费马小定理：可以把它看作是一个更一般的结果的特例, 但是当新的抽象概念没有发展起来以前, 甚至无法陈述这个更一般的结果.

这个抽象化过程有许多好处, 最明显的是它给了一个更一般的定理, 一个具有许多其他有趣的应用的定理. 一旦看到了这一点, 就能一下子证明一般的结果, 而不必分别证明各个特殊结果. 一个与之有联系的好处是, 它使我们能够看到, 许多

原来似乎无关的结果之间是有联系的. 而在数学的不同领域间找到联系几乎一定会影响这门学科的显著的进展.

3.3 鉴别出特征性质

定义 $\sqrt{2}$ 的方式和定义 $\sqrt{-1}$(通常都把它写作 i) 的方式成了明显的对照. 在前一情况, 如果我们小心的话, 先是证明确有一个正实数存在, 而且其平方为 2. 然后, 定义此数即为 $\sqrt{2}$.

对于 i, 这种风格的证明是不可能的, 因为没有哪个实数平方以后会等于 -1. 所以, 我们代之以另一个问题: 如果有一个数平方以后会等于 -1, 那么, 关于这个数有些什么可说? 这样一个数不可能是实数, 但这并未排除一种可能性, 就是扩张实数系为一个更大的数系, 使之能够包含 -1 的一个平方根.

初看起来, 似乎我们恰好是知道了关于 i 的一件事, 即 $\mathrm{i}^2=-1$. 但是如果还假设 i 服从算术的正常的法则, 就还可以做更多有趣的计算, 例如

$$(\mathrm{i}+1)^2=\mathrm{i}^2+2\mathrm{i}+1=-1+2\mathrm{i}+1=2\mathrm{i},$$

这意味着 $(1+\mathrm{i})/\sqrt{2}$ 是 i 的一个平方根.

从这两个简单的假设 —— 即 $\mathrm{i}^2=-1$ 以及 i 服从算术的通常法则 —— 就能发展起整个复数理论[I.3 §1.5] 而不必为 i 究竟是什么操心. 而事实上, 一旦停下来想一想 $\sqrt{2}$ 的存在性, 就会看到, $\sqrt{2}$ 的存在性其实并不如它的定义性质. [即借以定义 $\sqrt{2}$ 的性质]、那么重要, 而这个定义性质与 i 的定义性质, 即平方以后给出 -1, 是非常相似的, 这个定义性质就是平方以后给出 2, 以及服从算术的通常法则.

数学中许多重要的推广都是这样行事的. 另一个重要的例子是当 x 和 a 均为实数而 x 为正时 x^a 的定义. 除非 a 是正整数, x^a 这个表达式很难看出有什么意义, 然而, 不论 a 取什么值, 数学家们拿着这个表达式却好像没事人一样, 这是怎么回事呢? 答案在于, 关于 x^a, 真正要紧的不在于它取什么值, 而在于把它当作 a 的一个函数时, 它的特征性质是什么. [所谓特征性质, 不仅是说它所具有的性质, 而且是只要有了这个性质, 那就是它, 也就是仅有它才具有的性质]. x^a 的最重要的特征性质就是 $x^{a+b}=x^a x^b$, 有了这个性质, 再加上另外几个别的简单性质, 就完全确定了 x^a 这个函数. 这个例子将在条目指数和对数函数[III.25] 中作更详细的讨论.

抽象化和分类之间有着有趣的关系. "抽象" 这个词在数学中时常是指这样一部分数学, 在那里更经常使用一个对象的特征性质来进行讨论, 而不是直接从对象的定义来做论证 (虽然如 $\sqrt{2}$ 这个例子所表明的, 抽象和非抽象的区别时常有些模糊). 抽象的最终目的, 是从一组公理, 例如群或向量空间的公理, 开始来探讨其推论. 然而, 有时为了对这些代数结构进行推理, 对它们进行分类时常很有好处, 分类的结果是使它们变得更具体. 例如, 每一个有限维实向量空间 V 都同构于某个 $\mathbf{R}^n$,

而 n 是一个非负整数. 把 V 想作一个具体的 $\mathbf{R}^n$, 而不是想作一个满足某些公理的代数结构, 时常很有帮助. 于是, 在一定意义下, 分类是抽象化的对立面.

3.4 重新陈述以后再推广

维是一个在日常语言中也很熟悉的数学概念, 例如, 一把椅子的照片就是一个 3 维对象的 2 维表示, 因为椅子有高度、宽度和深度, 但是它的像只有高度和宽度. 粗略地说, 一个图形的维就是可以沿着它自由运动而始终停留在此图形内的独立的方向的个数, 这个粗略的概念可以在数学上搞精确 (利用*向量空间*[I.3 §2.3] 的概念).

如果给了一个图形, 则它的按正常理解的维应该是一个非负整数. 说我们可以在例如 1.4 个独立的方向上运动是没有意义的, 然而, 确实有一个分数维的严格的数学理论, 在这个理论中, 任意给一个非负实数 d, 都可以找到一个 d 维的图形.

数学家们是怎样做到这件似乎不可能的事情的呢? 答案是把这个概念重新陈述了, 只有那时, 才能推广它. 这句话的意思就是给维以一个具有以下性质的新的定义:

(i) 对于所有的 "简单的" 图形, 维的新定义和老定义一致. 例如在新定义下, 直线仍是 1 维的, 正方形仍是 2 维的, 立方体仍是 3 维的.

(ii) 在新定义下, 每个图形的维一定是正整数这一点不再是显然的.

做这件事有好几种方法, 但其中的绝大多数都集中在长度、面积和体积这些概念的差别上. 注意, 一条长度为 2 的直线段, 可以分成两个互不重叠的长度为 1 的直线段的并; 一个边长为 2 的正方形可以分成四个互不重叠的边长为 1 的正方形的并; 而一个边长为 2 的立方体, 可以分成八个互不重叠的边长为 1 的正方体之并. 因此, 若把一个 d 维图形按因子 r 放大, 则其 d 维 "体积" 会被乘上因子 r^d. 假设现在想展示一个 1.4 维图形. 方法之一是取 $r = 2^{5/7}$, 使得 $r^{1.4} = 2$, 然后找一个图形 X, 把它按因子 r 放大, 而且使得放大的图形可以分成两个互不相交的 X 的复本. X 的两个复本, 体积应该是 X 的 "体积" 的两倍, 所以 X 的维数 d 应该满足方程 $r^d = 2$. 按照我们对 r 的选择知道, X 的维数为 1.4. 详见*维*[III.17].

另一个初看起来没意义的概念是不可交换几何学. "交换" 这个词本来只用于*二元运算*[I.2 §2.4], 所以属于代数而不属于几何学, 那么, 不可交换几何学可能有什么意思呢?

但是现在, 答案已经不再令人惊奇了: 人们用某个代数结构来重新陈述几何学的一部分, 然后再推广这里的代数. 这个代数结构涉及到一个可交换的二元运算, 所以, 允许这个二元运算为不可交换的, 就推广了这个代数.

这里讲到的几何学的一部分就是*流形*[I.3 §6.9] 的研究. 与流形 X 相关的有定义在此流形 X 上的复值连续函数的集合 $C(X)$. 给出了 $C(X)$ 中的两个函数 f

和 g 以及两个复数 λ 和 μ, 则线性组合 $\lambda f+\mu g$ 仍是一个复值连续函数, 从而仍在 $C(X)$ 中, 所以 $C(X)$ 是一个向量空间. 然而, 还可以把 f 与 g 相乘 (定义为 $(fg)(x)=f(x)g(x)$). 这个乘法有各种自然的性质 (例如, 对于一切函数 f,g 和 h 有 $f(g+h)=fg+fh$), 这就使得 $C(X)$ 成为一个代数, 甚至是一个 C^*-代数[IV.15 §3]. 后来发现, 紧流形 X 上的相当大一部分几何学可以纯粹地以 C^*-代数 $C(X)$ 的语言来重新陈述. 这里的"纯粹地"这个词意味着并无必要讲到流形 X, 而 $C(X)$ 本来是参照着流形 X 来定义的 —— 我们需要的仅是 $C(X)$ 是一个代数. 这就意味着有可能有这样的不是几何地生成的代数, 但是对于它们, 经过重新陈述的几何概念仍然可用.

代数里有两个二元运算：向量空间运算和乘法[①]. 向量空间运算总是假设为可交换的, 但是乘法可不一定：如果乘法也是可交换的, 就说这个代数是可交换代数. 因为 fg 和 gf 显然是同一个函数, 代数 $C(X)$ 就是一个可交换 C^*-代数, 所以从几何学产生的代数总是可交换代数. 然而有许多几何概念在用代数语言重新陈述以后, 对于不可交换的 C^*-代数仍有意义, "不可交换几何学"这个词就这样使用起来了. 详见算子代数[IV.15 §5].

这样一种重新陈述以后再推广的程序在数学的许多最重要的进展中都有. 现在看本小节的第三个例子：算术的基本定理[V.14]. 顾名思义, 它是数论的基石之一, 它指出：每一个正整数都可以唯一的方式写成素数之积 ([当然, 这些素数因子的次序在这里是不予考虑的]). 然而数论专家总要看扩大的数系, 在绝大多数这类数系中, 算术的基本定理的明显的类似定理都是不成立的. 例如, 在形如 $a+b\sqrt{-5}$ 的数 (其中要求 a,b 为整数) 所成的环[III.81 §1] 中, 数 6 或者可以写成 2×3, 或者写成 $(1+\sqrt{-5})\times(1-\sqrt{-5})$. 因为 $2,3,1+\sqrt{-5},1-\sqrt{-5}$ 都不能进一步分解, 所以数 6 在此环中有两种真正不同的素因子分解.

然而, 有一种自然的方法推广"数"的概念, 使之包括理想数[III.81 §2], 这样, 就可以在例如刚才所述的那种环内, 证明算术的基本定理的一种版本. 首先把问题重新陈述如下：对每一个数 γ, 做所有倍数 $\delta\gamma$ 的集合, 其中 δ 是环中的元. 记此集合为 (γ), 具有以下的封闭性质：若 α,β 都属于 (γ), 而 δ,ε 都是此环中之元, 则 $\delta\alpha+\varepsilon\beta$ 也属于 (γ).

一个环的具有以上封闭性质的子集合, 就称为一个理想. 如果一个理想具有 (γ) 的形状, γ 是某个数, 则此理想称为一个主理想. 然而, 存在不是主理想的理想, 所以, 可以把理想的集合看成是推广了原来的环的元素的集合 (在这种推广下, 原来的元素 γ 看成主理想 (γ)). 结果是有自然的加法和乘法的概念可以适用于各个理想. 此外, 定义一个理想为"素"理想也是有意义的, 这里, 说理想 I 为素理想, 即

① 原书误为"加法与乘法".—— 中译本注

是指唯一地写 I 为两个理想 J, K 之积的方式是 J, K 中有一个是“单位元”. 在这个扩大的集合上因子的唯一分解定理是成立的. 这些概念给了一种非常有用的在原来的环中“量度因子分解的唯一性定理失效程度”的标尺. 更详细的讨论可见条目代数数[IV.1 §7].

3.5 更高的维数和多个变元

我们已经看到, 当不是只考虑单变元的一个方程, 而是考虑许多变元的方程组时, 多项式方程的研究会变得复杂得多. 我们已经看到了偏微分方程[I.3 §5.4], 它们可以看作是涉及多个变量的微分方程, 典型地, 分析它们会比分析常微分方程困难得多. 多变元的多项式方程组以及偏微分方程是一种过程的两个值得注意的例子, 这个过程就是从单变元推广到多变元, 产生了许多最重要的数学问题和结果, 特别是在 20 世纪以来.

设有一个涉及三个实变量 x, y 和 z 的方程. 把三元组 (x, y, z) 看成单独一个对象, 而不是三个数的一组, 这种想法时常是有用的. 此外, 这种对象有着自然的解释: 它代表 3 维空间的一点. 这个几何解释是重要的, 而且在很大程度上有助于说明为什么把许多定义和定理从一个变元推广到多个变元如此有趣. 如果把一项代数的工作从单变元推广到多变元, 就可以认为, 这是从 1 维的背景推广到高维的背景. 这个思想引导到代数与几何的许多联系, 使得来自一个领域的技巧可以用于其他领域.

4. 模式的发现

假设想用互不重叠的半径为 1 的圆盘把平面填充得尽可能紧密, 该怎么做? 这是所谓填充问题的一个例子. 答案已经知道, 而且正是如人们所期望的那样: 可以这样来排列这些圆盘, 使得它们的中心成为一个正三角形网格, 如图 1, 3 维情况下, 类似的结果也是对的, 但是难证多了. 直到最近, 它还只是一个未解决的问题, 并以“开普勒猜想”而闻名于世, 一直到了 1998 年, 才有一位美国数学家 Thomas Hales 宣称, 他借助于计算机得到了一个很长很复杂的解, 虽然他的解已经被证明是很难核验的, 但是有一个共识, 认为大概是正确的.

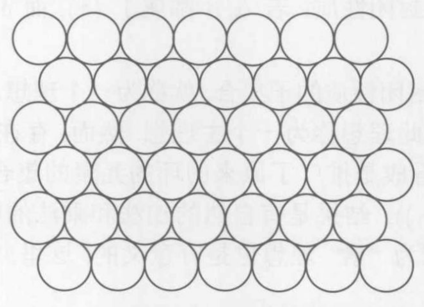


图 1 平面上圆盘的可能最紧密的排列

可以在任意维空间里提出球的填充问题, 但是随着维的增加, 这个问题变得越来越难. 说真的, 大概到了 97 维, 最紧密的填充将是永远不得而知的. 类似的经验提示, 最好的排列方法几乎绝不会有如同 2 维情况的那种简单结构了, 所以, 唯一的解决方法可能就是某种 "硬性搜寻"(brute-force search). 然而, 搜寻可能的最佳复杂结构是不可行的, 虽然能够想办法把这个过程化简为只在有限种可能性中搜索, 但这时可能性也还是为数太多, 使得实际搜寻成为不可行的.

对于一个看起来太难解决的问题, 不应该完全放弃. 一个更富成果的反应是提出一个有关联但是能够处理的问题. 对于现在的例子, 不必去发现最好的填充, 只需要看一下能够找到紧密到何种程度的填充. 下面在 n 相当大的时候, 概要地叙述在 n 维情况下, 能够给出相当好的填充的论据. 从极大填充开始, 所谓极大填充, 就是把球一个接一个地画进去, 但不要与已经画好的球重叠, 直到不与已经画好的球重叠就再也不能画新球为止. 现在, 令 x 为 $\mathbf{R}^n$ 的任一点. 这时, 在已经画好的球的集合中, 一定有一个球心与 x 的距离小于 2 的球, 因为否则就能够以这一点 x 为球心作一个单位球, 而它不会与任何一个画好的球相重叠. [所以, 这样作出的填充就是一个极大填充]. 至此, 取所有的球的集合, 并且把每一个球都按因子 2 放大, 就会把整个 $\mathbf{R}^n$ 覆盖起来. 因为把一个 n 维球按因子 2 放大时, 其 (n 维) 体积增加 2^n 倍, 所以未曾放大的球所已经覆盖的 $\mathbf{R}^n$ 的比例至少是 2^{-n}.

注意, 在以上的论证中, 对于紧密度达到 2^{-n} 的填充中球是如何排列的还一无所知. 我们所做的无非就是做出了一个极大填充, 做的方法也是相当随便的. 这与在 2 维情况下的方法成了鲜明的对照, 在 2 维情况下, 我们确实定义了圆盘的很独特的排列方式.

这样的对照在整个数学中比比皆是. 对于有些问题, 最好的处理途径是建立一个具有高度结构的模式, 使它具有所需要的性质, 而对于另一些问题 —— 这些问题想要得到精确的解通常是毫无希望 —— 去寻找不那么独特的安排反而更好. "具有高度结构的" 这个词, 这里就意味着 "具有高度对称性".

正三角形格网是一个很简单的模式, 但有些具有高度结构的模式却可能复杂得多, 而在发现它们时, 常会给人大得多的惊喜. 在填充问题中就有一个值得注意的例子. 大体说来, 研究的问题维数越高, 寻找好的模式就越困难, 但是这个一般的规律在 24 维的情况却发生了例外. 在这时出现了一个很不平常的构造, 称为利奇 (Leech) 格网, 给出了奇迹般紧密的填充. 形式地说, $\mathbf{R}^n$ 中的格网就是具有以下三个性质的子集合 Λ:

(i) 若 x 和 y 都属于 Λ, 则 $x+y$ 和 $x-y$ 也属于 Λ.

(ii) 若 x 属于 Λ, 则它必是孤立的. 就是说必定存在一个常数 $d>0$, 使 x 和 Λ 中任意其他点的距离至少是 d.

(iii) Λ 不包含于 $\mathbf{R}^n$ 的任意 $n-1$ 维子空间中.

$\mathbf{R}^n$ 中的所有具有整数坐标的点的集合 $\mathbf{Z}^n$ 就是格网的好例子. 如果要寻找一个紧密的填充, 关注于格网是一个好主意, 因为只要知道了格网中的每一个非零点距离 0 至少为 d, 则格网中任意两点的相互距离也至少为 d. 这是因为 Λ 中的 x 与 y 的距离, 与 $y-x$ 与 0 的距离是相同的. 所以, 不需要考虑整个格网, 只看它在 0 附近的那一部分就可以脱身了.

在 24 维情况下可以证明, 存在一个格网 Λ 具有以下的附加的性质, 这个格网在以下的意义下还是唯一的, 即所有也具有这些附加性质的格网都可以由这个 Λ 旋转而得.

(iv) 存在一个 24×24 矩阵 M, 其*行列式*[III.15] 等于 1, 而 Λ 就是 M 的各行的整数组合.

(v) 若 v 是 Λ 的一点, 则 v 到 0 的距离的平方是一个偶数.

(vi) Λ 中离 0 最近的非零向量的距离是 2. 所以, 以 Λ 的点为心半径为 1 的球, 构成 $\mathbf{R}^{24}$ 的一个填充.

离开 0 最近的非零向量远非唯一的, 事实上有 196 560 个, 考虑到这些点互相的距离为 2, 就可以看到这是一个非常大的数字, 这个格网就叫做利奇格网.

利奇格网有极大的对称性, 说准确一些, 有 8 315 553 613 086 720 000 个旋转对称 (这个数等于 $2^{22}\cdot 3^9\cdot 5^4\cdot 7^2\cdot 11\cdot 13\cdot 23$). 如果取这个对称群对于恒等元和负恒等元所成的子群的*商群*[I.3 §3.3], 就会得到康韦 (Conway) 群 Co_1, 它是*单群*[V.7] 的著名的散在子群之一. 有这么多对称性存在, 使得决定任意非零格点到 0 的距离更加容易, 因为只要核验了一个距离, 也就同时自动地核验了许多其他点的距离 (正如在正三角形格网情况下六重对称性使得 0 到 6 个相邻的非零点距离都相同). 关于利奇格网的这些事实表明了数学研究的一个一般原则: 若一个数学结构有了一个值得注意的性质, 也就会有其他性质. 特别是高度的对称性常与其他的有趣的特性有关. 于是, 如果说利奇格网的存在已经令人吃惊, 那么, 再发现它会给出 $\mathbf{R}^{24}$ 的极为紧密的填充就不太令人吃惊了. 事实上, 2004 年 Henry Cohn 和 Abhinav Kumar 表明, 它给出了 $\mathbf{R}^{24}$ 这个球的最紧的填充, 至少在格网给出的填充中, 它是最紧密的, 不过, 这一点仍未得到证明.

5. 解释表观上的偶合

最大的散在单群称为魔群. 这个名称部分地可以用它的大小来解释: 有 $2^{46}\cdot 3^{20}\cdot 5^9\cdot 7^6\cdot 11^2\cdot 13^3\cdot 17\cdot 19\cdot 23\cdot 29\cdot 31\cdot 41\cdot 47\cdot 59\cdot 71$ 个元素. 怎么能理解这么大的群呢?

最好的办法之一是证明它是某个其他的数学结构的对称群 (关于这个主题, 条目*表示理论*[IV.9] 讲了许多), 而且, 那个对象越小就越好. 我们刚才已经看到了另一个很大的散在单群, 康韦群 Co_1 与利奇格网的对称群有密切的关系. 是否也有某

个格网以魔群为对称群呢?

不难证明, 确实有一些格网能起作用, 但是更大的挑战是要找一个小维数的格网. 已经证明了最小可能的维数是 196 883.

现在转到一个不同的数学分支. 如果看一下关于代数数的条目 [IV.1 §8], 就会找到一个函数 $j(z)$ 的定义. 这个函数称为椭圆模函数, 它在代数数理论中起着中心的作用, 它是由一个级数的和来定义的, 这个级数是这样开始的:

$$j(z) = \mathrm{e}^{-2\pi iz} + 744 + 196\,884\mathrm{e}^{2\pi iz} + 21\,493\,760\mathrm{e}^{4\pi iz} + 864\,299\,970\mathrm{e}^{6\pi iz} + \cdots.$$

令人感兴趣的是级数中 $\mathrm{e}^{2\pi iz}$ 的系数是 196 884, 比刚才的格网的最小可能维数 196 883 只大了 1, 而这个格网是以魔群为对称群的.

并不明显的是我们应该多么严肃地对待这个观察, 当 John McKay 看到这一点时, 人们就已经有了分歧. 有人认为这大概只是偶合, 因为这两个领域看来如此不同而且互不相关. 另一些人的态度则是: 既然函数 $j(z)$ 和魔群在自己的领域中都如此重要, 而数 196 883 又这么大, 这种惊人的数值上的事实, 可能指向尚未发现的深刻联系.

后来证明第二种观点是正确的. 在研究了 $j(z)$ 的各个系数以后, McKay 和 John Thomson 提出了一个猜想, 即所有的系数 (不只是 196 884) 都与魔群有关. 这个猜想后来被康韦和 Simon Norton 扩展, 他们提出了所谓 "魔幻月光猜想" (monstrous moonshine conjecture), 在 1992 年被 Richard Borcherds 证明 (这里使用了 "月光" 二字, 说明开始时人们觉得魔群与 j 函数的联系朦胧如月色, 令人不敢相信).

Borcherds 为了证明这个猜想引进了一个新的代数结构, 并称之为*顶点代数*[IV.17], 而为了分析顶点代数, 他又利用了来自*弦论*[IV.17 §2] 的结果. 换句话说, 借助于理论物理学的概念, 他解释了两个看来很不相同的纯粹数学领域的联系.

这个例子用很极端的方式说明了数学研究的另一个一般原则: 如果能够从不同的数学来源, 得到同样的数字序列 (或者同样的更一般的数学结构), 那么这两个数学来源大概有点联系, 不会如初看时觉得的那样互不相关. 此外, 如果能够找到一个深刻的联系, 说不定就会被引到其他深刻联系. 有许多别的例子, 其中完全不同的计算给出了相同的答案, 而至今未得解释. 这些现象后来成了数学中的某些最困难最吸引人的未解决问题 (请看对于*镜面对称*[IV.16] 的介绍, 其中有另一个例子).

更有趣的是, j 函数还引到了第二个著名的数学 "偶合". 数 $\mathrm{e}^{\pi\sqrt{163}}$ 大概没有什么特别的地方, 但是它的十进小数展开是这样开始的:

$$\mathrm{e}^{\pi\sqrt{163}} = 262\,537\,412\,640\,768\,743.999\,999\,999\,999\,25\cdots.$$

[注意, 小数点后紧接着 12 个 9]. 它与一个整数 262 537 412 640 768 744 如此惊人地接近, 二者只相差不到 2×10^{-13}! 开始的时候, 这件事又一次诱使人把它只当成

一个偶合, 但是, 屈服于一个诱惑之前, 必须三思而行! 毕竟不会有很多的数定义可以如 $e^{\pi\sqrt{163}}$ 一样简单, 而其接近于一个整数的程度也如 $e^{\pi\sqrt{163}}$ 那样. 事实上, 这完全不是偶合, 关于其解释, 可见代数数[IV.1 §8] ①.

6. 计数与量度

正二十面体有多少个旋转对称? 下面是一个计算的方法. 选择正二十面体的一个顶点 v, 令 v' 是其相邻顶点之一. 一个正二十面体有 12 个顶点, 所以在旋转以后, v 可以停留在这 12 个地方. 在知道了 v 的去处以后, v' 还有 5 个可能的地方去 (正二十面体的每一个顶点有 5 个相邻的顶点, 而 v' 在旋转以后仍然与 v 相邻). 在 v 和 v' 的去处确定了以后, 再也没有其他选择了, 所以选中对称的总数是 $5 \times 12 = 60$.

这是计数论证的一个简单例子, 即回答 "有多少个" 这种问题的答案. 然而, "论证" 一词至少和 "计数" 一样重要, 因为并不是把所有的对称排成一排, 然后 "1, 2, 3, $\cdots$, 60" 这样数下去, 而在实际生活中是可能这样去数的. 相反, 我们是提出了选中对称的总数为 5×12 的一个理由. 在这个过程结束之时, 我们对于这种对称的了解也超过了仅只知道其总数. 事实上, 还可以前进一步, 证明正二十面体的旋转群为 A_5, 即含有 5 个元素的交错群[III.68].

6.1　准确计数

下面是一个比较精巧的计数问题. 一个 n 步的 1 维随机游动就是一串整数 $a_0, a_1, a_2, \cdots, a_n$, 使得差 $a_i - a_{i-1}$ 或者为 1 或者为 -1. 例如, $0, 1, 2, 1, 2, 1, 0, -1$ 就是一个 7 步的随机游动. 从 0 开始的 n 步随机游动的总数为 2^n, 因为每一步都有两种选择 (加 1 或者减 1).

现在试一个稍微复杂的问题. 有多少长度为 $2n$ 的起点与终点都在 0 处的随机游动? (我们看长度为 $2n$ 的游动, 是因为起点和终点相同的随机游动必有偶数步).

为了思考这个问题, 用 R 和 L(分别表示 "右" 和 "左") 代替加 1 和减 1. 这就给出了从 0 开始的随机游动另一种记法, 例如上面的游动 $0, 1, 2, 1, 2, 1, 0, -1$ 现在就可以记为 RRLRLLL. 一个从 0 开始的随机游动终点也在 0 处的充分必要条件是 R 的个数与 L 的个数相同. 此外, 如果知道了 R 的位置, 也就知道了整个游动. 所以, 要计数的总数就是在 $2n$ 步中选取 n 步为 R 的选取方式的个数, 大家知道这是 $(2n)!/(n!)^2$.

现在来看一个相关的量, 但是要决定它就颇不容易了, 这就是步长为 $2n$ 从 0 开始也到 0 为止, 但是过程中不能取负值的随机游动的总数 $W(n)$. 这个问题用上一个问题 $(2n = 6)$ 的记号来写, 就是要求列出所有的长度为 6 的随机游动, 它们

① 这段话是译者加的. —— 中译本注

是: RRRLLL, RRLRLL, RRLLRL, RLRRLL, 以及 RLRLRL, 一共有 5 个游动.

这 5 个游动中有 3 个不仅是从 0 开始也到 0 结束, 而且在过程中还访问过 0 一次, RRLLRL 在第 4 步后访问了 0; RLRRLL 在第 2 步后访问了 0; RLRLRL 在第 2 步和第 4 步后都访问了 0. 假设长为 $2n$ 的游动直到第 $2k$ 步以后才第一次访问 0, 于是 $2k$ 步以后余下的部分就是一个包含 $2(n-k)$ 步从 0 开始也到 0 结束, 且过程中绝不为负的游动, 这种游动共有 $W(n-k)$ 个. 至于前面的 $2k$ 步, 除了起始一步是从 R 起, 最后一步是到 L 止, 中间还有 $2(k-1)$ 步是从 1 起, 到 1 止, 而且过程中不会有小于 1 的游动. 这种游动的个数显然与 $W(k-1)$ 相同. 这样, 因为第一次访问 0 必定是在第 $2k$ 步后发生, 这里 k 在 1 和 n 之间, 所以 $W(n)$ 必满足稍微复杂一点的递归关系

$$W(n)=W(0)W(n-1)+\cdots+W(n-1)W(0),$$

其中应该取 $W(0)=1$.

这就使我们能够计算出前几个 W 值, 有 $W(1)=W(0)W(0)=1$, 其实这个情况直接来看更加容易, 因为这种游动只能是 RL. 然后, $W(2)=W(1)W(0)+W(0)W(1)=2$. 再就是 $W(3)$, 也就是上面说的那一种 6 步游动的个数, 等于 $W(2)W(0)+W(1)W(1)+W(0)W(2)$, 也就是 5, 于是证实了刚才的计算.

当然, 如果想对大的 n, 例如 $n=10^{10}$, 算出 $W(n)$, 直接利用递归公式就不是一个好主意了. 然而这递归关系的形式相当漂亮, 可以用*生成函数*[IV.18§§2.4, 3] 来处理, 这一点在条目*列举组合学与代数组合学*[IV.18§3] 中有讨论 (为了看出这里的问题与那里的讨论的关系, 把字母 R 和 L 分别代以方括号 "[" 和 "]". 于是一个合法的方括号记法就相当于一个永不为负的随机游动).

以上的论证给出了一个精确计算出 $W(n)$ 的有效方法. 数学中有许多别的准确计算论证的例证, 下面仅仅给出 4 个例证, 它们只是一个小小的样本, 数学家们知道怎样精确计算这个样本里所选定的问题里的量, 而不必求助于 "硬算"(请看 [IV.18] 的引言, 其中讨论到一个计数问题怎样就算是解决了).

(i) 平面被 n 条直线分割开所成的区域的数目 $r(n)$, 但这些直线中没有平行的, 也没有三条直线共点. 对于 $n=1, 2, 3, 4$, $r(n)=2, 4, 7, 11$. 不难证明 $r(n)=r(n-1)+n$, 由此即可导出 $r(n)=n(n+3)/2$. 这个命题及其证明可以推广到高维情况.

(ii) 把 n 写为四个平方和的方法的数目 $s(n)$. 在这个问题中, 允许把零和负数的平方都算进去, 而且把不同次序的写法都算是不同的结果 (所以, 例如 $1^2+3^2+4^2+2^2$, $3^2+4^2+1^2+2^2$, $1^2+(-3)^2+4^2+2^2$, 还有 $0^2+1^2+2^2+5^2$, 都要算作把 30 写为四个平方之和的四种不同方法). 可以证明, $s(n)$ 等于 n 的那些不是 4 的倍数的因子的和数再乘以 8. 例如 12 以 1, 2, 3, 4, 6, 12 为因子, 其中 1, 2,

3, 6 不是 4 的倍数, 所以 $s(12) = 8(1+2+3+6) = 96$, 其中的不同方法就是由 $1^2+1^2+1^2+3^2, 0^2+4^2+4^2+4^2$ 以不同方法对各项重排次序, 或把正整数换成负整数得到的各个平方和.

(iii) 如何计算空间 $\mathbf{R}^3$ 中与四条给定直线 L_1, L_2, L_3 和 L_4 都相交的直线的数目. 这里要求这四条直线处于"一般位置"(所谓"一般位置"就是说这四条直线 [的相互位置] 没有特别之处, 例如要求其中两条要平行, 或要求所有这些直线都要彼此相交, [而不能有中学立体几何课里讲的"异面直线"之类的情况], 如此等等, 都不叫"一般位置"). 有这样的结果, 通过任意三条这样的直线, 必有 $\mathbf{R}^3$ 中的一个二次曲面 (quadric surface), 而且这个二次曲面是唯一的. 现在过 L_1, L_2, L_3 作一个二次曲面, 记为 S.

这个曲面有一些有趣的性质, 可以用来解决我们的问题. 主要的性质就是可以找到直线的连续族 (即直线的一个集合 $L(t)$ 使得每一个 t 对应于一直线, 而且此直线对 t 为连续的), 它们共同构成了曲面 S, 而且包括了 L_1, L_2, L_3 中的每一个. 此外, 还有另外一个连续的直线族 $M(s)$, 使其中每一条直线均与 $L(t)$ 的每一条直线相交. 当然也会与 L_1, L_2, L_3 都相交, 而每一条同时与 L_1, L_2, L_3 都相交的直线也都包含在 $M(s)$ 中.

可以证明, L_4 必定与 S 恰好交于两点 P, Q. P 位于第二族直线的某一条 (设为 $M(s)$) 上, Q 则位于另一条 $M(s')$ 上 (这一条必与 $M(s)$ 不同, 否则, L_4 就是 $M(s)$, 而与 L_1, L_2, L_3 都相交, 这与 L_1, L_2, L_3 和 L_4 处于一般位置相矛盾). 所以, 这两条直线 $M(s)$ 和 $M(s')$ 与所有四条直线 L_i 都相交. 但是与所有四条 L_i 都相交的直线必定属于 $M(s)$, 从而必定通过 P, Q 中的某一点 (因为 $M(s)$ 的直线都位于 S 上, 而 L_4 又与 S 仅交于这两点). 所以, 与所有四条直线 L_i 都相交的直线的条数为 2.

这个问题可以有相当大的推广, 而且可以用一种称为 Schubert 计算 (calculus) 的技巧来解决.

(iv) 设正整数 n 可以用 $p(n)$ 种方法来表示为正整数之和. 例如当 $n = 6$ 时, $p(6) = 11$, 因为有 $6 = 1+1+1+1+1+1 = 2+1+1+1+1 = 2+2+1+1 = 2+2+2 = 3+1+1+1 = 3+2+1 = 3+3 = 4+1+1 = 4+2 = 5+1 = 6$. 函数 $p(n)$ 成为分割函数. 哈代[VI.73] 和拉玛努金[VI.82] 给出了 $p(n)$ 的一个非常好的逼近函数 $\alpha(n)$, 准确到 $p(n)$ 就是最近于 $\alpha(n)$ 的整数.

6.2 估计

看见了上面的例 (ii), 就会想到它可否推广. 例如, 有没有一个公式可以给出把 n 写成 10 个六次方之和的方法之数目 $t(n)$? 一般都相信答案为"否", 至少可以肯定这个公式至今也未找到. 然而, 和填充问题一样, 哪怕准确的答案不一定很快会被找到, 找到它的估计也是非常有趣的. 这就要去定义一个容易计算的函数 f, 使

得 $f(n)$ 总是近似地等于 $t(n)$. 如果这还是太难, 可以试着去找两个容易计算的函数 L 和 U, 使得对于一切 n 都有 $L(n) \leqslant t(n) \leqslant U(n)$. 如果成功了, 就称 L 为 t 的下界, 而称 U 为上界. 下面举几个量为例, 没有人知道怎样精确地对它们计数, 但是它们都有有趣的逼近, 至少是有有趣的上界和下界.

(i) 在整个数学中最著名的估计问题可能就是 $\pi(n)$ 的估计. 这里的 $\pi(n)$ 就是小于或等于 n 的素数的个数. 对于小的 n, 当然可以精确地算出 $\pi(n)$ 来, 例如 $\pi(20)=8$, 因为小于或等于 20 的素数有 8 个: 2, 3, 5, 7, 11, 13, 17 和 19. 然而, $\pi(n)$ 似乎没有一个有用的公式, 虽然可以设想一个硬算 $\pi(n)$ 的 "强力"(brute-force) 算法 —— 就是从小到大, 逐个数地检验是否为素数, 一直到 n 为止 —— 但是对于大的 n, 这个程序耗时之多使得无法实行. 此外, 这个办法对于函数 $\pi(n)$ 的本性, 不能增加什么新的洞察.

但是, 如果把问题稍作改变, 只是问, 到 n 为止大体上有多少素数, 就进入了所谓的*解析数论*[IV.2] 这个领域, 这是一个包含了许多吸引人的结果的数学领域. 特别是由*阿达玛*[VI.65] 和*瓦莱 · 布散*[VI.67] 在 19 世纪末证明的著名的*素数定理*[V.26] 指出, $\pi(n)$ 近似等于 $n/\log n$, 这里的近似等于的意义是 $\pi(n)$ 与 $n/\log n$ 之比当 n 趋近无穷大时趋于 1.

这个命题还可以更加精确化. 在靠近 n 处, 素数的密度大约是 $1/\log n$, 意思是在 n 附近随机地选取一个整数, 恰好是素数的概率是 $1/\log n$. 这就提示, $\pi(n)$ 大概是 $\int_0^n \mathrm{d}t/\log t$. n 的这个函数称为对数积分, 记号是 $\mathrm{li}(n)$.

这个估计精确度如何? 谁也不知道. 但是, *黎曼假设*[V.26](这大概是数学里最著名的未解决的问题) 等价于以下命题: $\pi(n)$ 和 $\mathrm{li}(n)$ 相差最多是 $c\sqrt{n}\log n$, 这里的 c 是某个常数. 因为 $\sqrt{n}\log n$ 比 $\pi(n)$ 要小得多, 这就说明 $\mathrm{li}(n)$ 是 $\pi(n)$ 的极好的近似.

(ii) 所谓平面上的长度为 n 的自身回避游动就是具有以下性质的一串点 $(a_0,b_0),(a_1,b_1),(a_2,b_2),\cdots,(a_n,b_n)$:

- 数 a_i , b_i 都是整数.
- 对于每一个 i, 从 (a_{i-1},b_{i-1}) 到 (a_i,b_i) 总是沿水平方向或竖直方向移动长度为 1 的一步, 即或者 $a_i=a_{i-1}, b_i=b_{i-1}\pm 1$, 或者 $a_i=a_{i-1}\pm 1, b_i=b_{i-1}$.
- 没有两个相同的点 (a_i,b_i).

前两个条件说明这个点序列构成一个长度为 n 的 2 维的游动, 第三个条件说明这个游动绝不会多于一次地访问同一点, "自避游动" 一词就由此而来.

令长度为 n 从 $(0,0)$ 开始的自身回避游动的总数为 $S(n)$. 至今不知道它的公式, 而且也不像是存在这么一个公式. 然而, 关于 n 变大时它是如何增长知道得并不少. 例如, 很容易证明 $S(n)^{1/n}$ 收敛于一个常数 c. c 的值是多少并不知道, 但是

已经 (借助于计算机) 知道, 它大概在 2.62 和 2.68 之间.

(iii) 令 $C(t)$ 是位于中心在原点半径为 t 的圆内的坐标为整数的点的个数. 就是说, $C(t)$ 是适合条件 $a^2+b^2 \leqslant t^2$ 的整数对 (a,b) 的个数. 半径为 t 的圆, 面积为 πt^2, 而平面可以用坐标为整数的点为中心的单位正方形铺满. 所以当 t 很大时, 很清楚 (也不难证明)$C(t)$ 近似地就是 πt^2. 然而, 这个近似好到什么程度就不那么清楚了.

为使这个问题变得比较明确, 令 $\varepsilon(t)=|C(t)-\pi t^2|$, 就是说 $\varepsilon(t)$ 表示用 πt^2 作 $C(t)$ 的估计时所产生的误差. 1915 年, 哈代和兰道 (Edmund Georg Hermann Landau, 1877—1938, 德国数学家) 证明了 $\varepsilon(t)$ 必至少是 $c\sqrt{t}, c>0$ 是一个常数, 而这个估计, 或者某个很类似的东西, 给出了 $\varepsilon(t)$ 的正确的数量级. 然而, 现在知道的最好的上界是由 Huxley 在 1990 年给出的: $\varepsilon(t)$ 最多是 $At^{46/73}, A$ 是一个常数. 这是很长的一连串改进中最新的一个.

6.3 平均

迄今我们的讨论限于计数某一种数学对象时的估计和近似. 然而, 绝不是只在这样的场合估计才是有意思的. 给定了对象的一个集合, 我们可能不仅是对这个集合有多大感兴趣, 而且还对这个集合的典型对象是什么样有兴趣. 这类问题有许多都具有下面的形式, 即某个与每个对象都有关的数值参数的平均值如何. 下面有两个例子:

(i) 一个步数为 n 的自避游动从起点到终点的平均距离 $S(n)$①是什么. 在这个问题里面, 对象就是从 $(0,0)$ 开始的步数为 n 的自避游动, 数值参数就是由起点到终点的距离.

令人吃惊的是, 这个问题难得出了名, 关于它几乎是一无所知. 显然, n 是 $S(n)$ 的一个上界, 但是我们可以预期, 一个典型的自避游动有许多扭曲转折, 所以在旅行结束时, 到起点的距离会远小于 n. 然而, $S(n)$ 一直也没有实质上比 n 更好的上界.

从另一个方向来看, 一个典型的自避游动的从起点到终点的距离会大于普通游动从起点到终点的距离, 这样才会留下充分的空间让这个游动自身回避. 这就提示 $S(n)$ 会显著地大于 $\sqrt{n}$, 但是就连简单地大于 $\sqrt{n}$ 也没有证到.

然而事情还远不止于此, 在 §8 中还会进一步讨论这个问题.

(ii) 令 n 为一随机选择的正整数, 而 $\omega(n)$ 为 n 的不同的素数因子的个数. $\omega(n)$ 平均会有多大? 事实是, 这个问题没有什么意义. 因为正整数的数目无穷, 无法随机地选取某一个. 然而, 若指定一个正整数 m, 而在 m 和 $2m$ 之间选取一个随机整数 n, 这就把问题弄精确了. 结果是: $\omega(n)$ 的平均大小是 $\log\log n$.

事实上, 我们知道的远远多于这些, 如果说对于随机变量[III.71 §4] 只是知道其

① §6.2 的第二个例子中也用了符号 $S(n)$, 但是明显地不是这里说的平均距离. 这里提醒一下, 以防混淆.—— 中译本注

平均值, 对其性态还大多不知, 所以, 对于许多问题, 计算平均值还只是事情的开始. 在这个情况, 哈代和拉玛努金给出了 $\omega(n)$ 的标准偏差[III.71 §4], 表明了它大概是 $\sqrt{\log\log n}$. 后来, 爱尔特希 (Erdös) 和 Kac 走得更远, 精确估计了 $\omega(n)$ 与 $\log\log n$ 相差大于 $c\sqrt{\log\log n}$ 的概率, 证明了一个惊人的事实, 即 $\omega(n)$ 的分布接近于高斯分布[III.71 §5].

看一看这些结果的展望, 我们来想一想 $\omega(n)$ 的可能值的域. 从一个极端情况看, n 本身可能就是一个素数, 这时它显然只有一个素因子. 在另一极端, 把素数按上升次序写为 $p_1, p_2, p_3, \cdots$ 而取 $n = p_1p_2\cdots p_k$ 的形式. 用素数定理可以证明: k 的数量级为 $\log n/\log\log n$, 这就比 $\log\log n$ 大得多. 然而上面的结果告诉我们, 这种形式只是例外的情况, 一个典型的数只会有很少几个不同的素因子, 而不会有 $\log m/\log\log m$ 那么多.

6.4 极值问题

数学中有许多问题, 要求在各种约束之下, 使某个量最大化或最小化, 这些问题称为极值问题. 和计数问题一样, 有一些极值问题可以实际地算出精确解来, 而更多的则是, 虽然精确解是谈不上的, 但仍然可以找到有趣的估计. 这两类问题, 下面各有一些例子.

(i) 令 n 为一正整数, 而 X 为一含有 n 个元素的集合. 问可以找出 X 的多少个子集合, 使得没有一个会含于另一个子集合之内.

可以做出的一个简单观察是: 如果两个不同子集合大小相同, 则没有一个会包含于另一个之内. 所以满足问题的约束的方法之一是选取所有的子集合具有同样大小 k. X 的大小为 k 的子集合一共有 $n!/k!(n-k)!$ 个, 这个数通常记为 $\binom{n}{k}$(或 ${}^nC_k$), 而不难证明当 $k = n/2$(若 n 是偶数) 或者 $k = (n\pm1)/2$(若 n 是奇数) 时, 它取最大值. 为简单计, 我们集中于 n 为偶数的情况. 刚才证明了: 在 n 元素的集合中, 可以做出 $\binom{n}{n/2}$ 个 $n/2$ 元素的子集合, 其中没有一个会包含任意另一个. 也就是说, $\binom{n}{n/2}$ 是这个问题的一个下界. 一个称为 Sperner 定理的结果指出, 它也是一个上界. 就是说, 如果取多于 $\binom{n}{n/2}$ 个子集合, 不论怎样取, 其中必有一个包含于另一个之内 (如果 n 是奇数, 答案如人们可以预期的那样, 将是 $\binom{n}{(n+1)/2}$).

(ii) 设有一条有重量的链子, 两端挂在天花板的两个钩子上, 而除此以外链子

再没有其他支撑点. 这个挂着的链子将是什么形状?

初看起来, 这并不像是一个极大极小问题, 但它很快就会变成一个. 这是因为物理学的一个一般原理告诉我们, 链子将会静止在一个使得位能为最小的形状上. 这样我们就面临一个新问题：令 A , B 是 [位于同一水平高度而] 相距的距离为 d 的两点, $\mathcal{C}$ 为长度为 l 以 A , B 为两端的曲线的集合, 问哪一条曲线 $C \in \mathcal{C}$ 具有最小位能? 这里设任意曲线段的质量正比于其长度. 这条曲线的位能是 mgh, m 是曲线的质量, g 是引力常数, 而 h 为曲线的重心的高度. 因为 m 和 g 不会改变, 这个问题就有了一个新的陈述：哪一条曲线 $C \in \mathcal{C}$ 具有最小的平均高度?

这个问题可以用一种称为变分法的技术来解决. 粗略地说, 它的思想是：有了一个集合 $\mathcal{C}$, 又有了一个定义在 $\mathcal{C}$ 上的函数 h, 即平均高度, 此函数把每一个 $C \in \mathcal{C}$ 映为其平均高度. 我们试着来使 h 最小化, 而处理这个问题的一个自然的途径是设法定义某种导数, 然后再去找一条曲线 $C \in \mathcal{C}$, 使得这个导数为 0. 注意, "导数" 一词在这里并不是沿着曲线运动时高度的变率, 而是指曲线的平均高度 (以线性方式) 对于整个曲线的微小摄动的响应. 利用这一类的导数来求最小值, 比求定义在 $\mathbf{R}$ 上的函数的驻点要复杂一点, 因为 $\mathcal{C}$ 是一个无限维的集合, 所以比 $\mathbf{R}$ 要复杂得多. 然而这个途径还是能起作用的, 解也是知道的, 是一种称为悬链线 (catenary, 此词来自拉丁文, 就是链子的意思) 的曲线. 这是又一个能够准确回答的最小化问题.

变分法的典型问题都是求一条曲线、一个曲面或者更一般种类的函数, 使得某一个量达到最大或最小值. 如果这个最大或者最小存在 (对于一个无限维集合, 它们绝非自动存在的), 则使得最大或最小达到的对象, 会满足一组偏微分方程 [I.3 §5.4], 称为欧拉–拉格朗日方程. 关于这种类型的最小化与最大化问题, 详见变分法[III.94] (亦见优化与拉格朗日乘子[III.64]).

(iii) 在 1 和 n 之间可以找到多少个数, 使得其中不会有 3 个构成等差数列? 如果 n=9, 答案是 5. 为了看到这一点, 首先注意, 在 1, 2, 4, 8, 9 这五个数中, 找不到 3 个成为等差数列. 所以, 在 1 到 9 之间有五个数, 其中没有等差数列. [那么, 在 1 到 9 之间能否找到 6 个数使其中不会有 3 个数的等差数列呢? 这也不会. 原因如下：]

如果这 6 个数中已经包含了 5, 那么必须舍去 4 或 6. 否则, 4, 5, 6 就是 3 个数的等差数列. 类似地, 必须舍去 3 与 7 之一, 2 与 8 之一, 1 与 9 之一. 总之要舍去 4 个数, 而只剩下 5 个, 与题设的 6 个数发生矛盾. 总之, 这 6 个数中不能有 5 在.

我们又必须舍去 1, 2, 3 中的一个数, [如果一个都不舍, 则又出现了等差数列 1, 2, 3], 同理也必须舍去 7, 8, 9 中的一个. [但是, 我们已经不许可取 5], 所以 4 和 6 都必须保留. 但是那样一来, 就不能保留 2 或 8. 也必须舍去 1, 4, 7 之一, 总之必须舍去至少 4 个数, [而不可能留下 6 个数].

当 n=9 时, 这种笨拙的逐个情况逐一论证的办法还算行得通, n 稍微大一点,

个别情况的数目就太大,而无法逐一考虑了.对于这个问题,似乎没有一个干净利落的答案准确地告诉我们,在 1 到 n 之间最大的不包含长度为 3 的等差数列的集合是什么,所以我们代之以寻求这个集合的大小的上下界.为了证明一个下界,必须找到一个好的构造、一个不包含任意等差数列大集合的方法;而为了证明一个上界,就必须证明:任意的有一定大小的集合,必定含有一个等差数列.至今为止,离最佳的界还很远呢.1947 年,Behrend 找到了一个大小为 $n/\mathrm{e}^{c\sqrt{\log n}}$ 的集合,其中没有等差数列,而在 1999 年 Jean Bourgain 又证明了每一个大小为 $Cn\sqrt{\log\log n/\log n}$ 的集合都含有一个等差数列 (如果还不清楚这两个数相距甚远,请看当 $n=10^{100}$ 时,这两个数各为多少.这时,$\mathrm{e}^{\sqrt{\log n}}$ 约为 4 000 000,而 $\sqrt{\log n/\log\log n}$ 约为 6.5).

(iv) 理论计算机科学是许多最小化问题的来源:当人们编制一个计算机程序以完成一项任务时,他就会希望在尽可能短的时间里完成它.下面是一个听起来很初等的例子:如果想把两个 n 位数相乘,需要多少步?

即令对于什么叫做一"步"并不太清楚,也能看到通常的乘法,即长乘法,至少需要 n^2 步.这是因为在计算过程中,第一个数的每一位都会被第二位数的每一位去乘.人们可能心想,这是必不可少的,但是事实上,有聪明的方法把问题变换一下,就能极大地减少计算机完成这类乘法所需的时间.最快的方法是用快速傅里叶变换 [III.26] 来把计算的步数从 n^2 减少到 $Cn\log n\log\log n$.因为一个数的对数远小于这个数本身,我们就会觉得 $Cn\log n\log\log n$ 只不过是比 Cn 形式的界稍微差一点.后面这种形式的界称为线性的,而对于这样的问题,这种线性的界显得是最好的了,因为哪怕是把这两个数的各位读一遍也需要 $2n$ 步.

另一个实质上类似的问题是:矩阵乘法有没有快速算法?要想用显然的方法把两个 $n\times n$ 矩阵乘起来,需要对矩阵里面的数作 n^3 次单个的乘法.这个问题上的突破主要来自 Strassen,他的思想是把这两个 $n\times n$ 矩阵的每一个都"平分"成 4 个 $\frac{n}{2}\times\frac{n}{2}$矩阵再相乘.初看起来只不过是把原来矩阵的乘法化为 8 对小矩阵的乘法,但是这些乘法实际上是互有关联的,Strassen 做了 7 个乘法,而 8 个乘法就可以由此导出了.然后就可以利用递归,就是把同样的思想用于加速这 7 个 $\frac{n}{2}\times\frac{n}{2}$ 矩阵的乘法,并仿此以往.

Strassen 的算法把矩阵乘法的步数的数量级从 n^3 降为 $n^{\log_2 7}$.因为 $\log_2 7<2.81$,所以这已经是显著的改进,不过要当 n 很大时才是.他的基本的分而治之的策略后来又得到改进,当前的记录已经是 $n^{2.4}$.从另一个方向来看,这个结果尚不能令人满意,因为谁也没有证明过,步数必须要显著地超过 n^2.

关于更多的这一类问题,可见计算复杂性[IV.20] 和算法设计的数学[VII.5].

(v) 还有一类更加微妙的最大化和最小化问题.例如,假设我们想要理解相继的素数之差的性质.这种差最小为 1(2 和 3 之差),不难证明差没有最大的 (给定任意大于 1 的正整数 n,则在 $n!+2$ 与 $n!+n$ 之间的数没有一个会是素数),所以关

于这些差似乎不会有有趣的最大化和最小化问题.

然而事实是, 如果先作适当的规范化, 就可以提出很吸引人的问题. 我们在本节前面提到过, 素数定理指出, 接近于 n 的素数, 密度是大约 $1/\log n$, 所以 n 附近的两个素数间平均的空隙长约为 $\log n$. 如果 p, q 是两个相继的素数, 就可以定义它们的规范化的空隙长为 $(q-p)/\log p$. 这个规范化空隙长的平均值为 1, 但是会不会有时小得多, 有时又大得多?

Westzynthius 在 1931 年就指出, 甚至规范化空隙长也可能任意长, 广泛的信念则是它也可以任意接近于 0(由著名的孪生素数猜想 —— 即有无穷多个素数 p 使得 $p+2$ 同时也是素数 —— 立刻可以推出这件事), 然而一直到 2005 年, 才由 Goldston, Pintz 和 Yildirim 证明了这一点 (条目*解析数论*[IV.2 §§6–8] 对此有较详细的讨论).

7. 判定不同的数学性质为相容

为了理解一个数学概念, 例如群或流形, 人们典型地要经历不同的阶段. 很明显, 从熟悉这个结构的几个代表性的例子开始, 也从学会由老例子建立起新例子的技巧开始, 这些都是好主意. 特别重要的是要了解由这个结构的一个例子到另一个例子的同态, 即 "保持结构的函数". 这一点在*一些基本的数学定义*[I.3 §§4.1, 4.2] 中讨论过.

一旦了解了这些基本之点, 还需要了解什么? 一个一般理论要想有用, 就必须就某些特定的例子告诉我们什么. 例如, 在 §3.2 中, 拉格朗日定理被用来证明费马小定理. 拉格朗日定理是关于群的一个一般事实: 若 G 是一个群, 其大小为 n, 则其任意子群的大小必是 n 的一个因子. 要想得到费马小定理, 就需要把拉格朗日定理用于 "G 为非零整数关于 mod p 的乘法所成的群" 这个特例. 我们得到的结论 —— $a^p \equiv a \bmod p$ —— 远非显然的.

然而, 如果关于群 G 我们想要知道一点对于一般群并不一定为真的什么事情, 又该怎么办呢? 就是说, 现在我们想要判定, G 是否具有一个某些群具有某些群则不具有的性质 P. 既然这个性质是不能从群的公理导出的, 看来似乎应该放弃群的一般理论, 而只来看特定的群 G. 然而, 在很多情况下, 还有一种介乎其间的可能性: 对于群 G, 去鉴识它是否具有一个 "相当一般" 的性质 Q, 再看能否从 Q 导出我们关心的性质 P.

下面是这一类方法在不同背景下的一个例子. 假设我们想要确定以下的多项式是否有一个实根: $p(x) = x^4 - 2x^3 - x^2 - 2x + 1$. 方法之一是去研究这个特定的多项式, 试着找出它的一个实根来. 例如, 在花了一番力气以后, 我们可能会发现 $p(x)$ 可以因式分解为 $(x^2+x+1)(x^2-3x+1)$. 第一个因子恒为正, 但是用二次方程公式于第二个因子, 我们发现, 当 $x = (3 \pm \sqrt{5})/2$ 时 $p(x) = 0$. 另一个方法则要用一

点一般理论：注意到 $p(1)$ 为负 (实际上为 -3), 而当 x 很大时, $p(x)$ 也很大 (因为 x^4 这一项远大于其他所有项), 然后再用中间值定理 (若一个连续函数有时为正, 有时为负, 则必在中间某点为零) 就行了.

注意, 在第二种方法里, 仍然需要某些计算 —— 找出 x 的一个值, 使得 $p(x)$ 为负 —— 但是它比第一个方法里的计算 —— 找出 x 的一个值, 使得 $p(x)$ 为零 —— 要简单得多. 在第二种方法里, 我们是去证明 $p(x)$ 仍然具有一个 "相当一般" 的性质, 即在某处为负, 然后再用中间值定理结束论证.

在整个数学里这样的情况很多, 在这些情况里, 证明某一个一般的性质是特别有用的. 例如, 已经知道一个正整数 n 是素数, 或者知道某一个群 G 是阿贝尔群 (即对 G 中任意两个元 g,h 均有 $gh=hg$), 或者知道某一个映复数为复数的函数是全纯函数[I.3 §5.6], 然后就能作为这些一般性质的推论, 关于这个对象, 知道更多的东西.

当这些性质已经确定是重要性质时, 它们就会给出一大类数学问题, 其形式如下：给定一个数学结构, 并选择一些它可能具有的有趣性质, 这些性质有哪些组合会蕴含其他性质？并非所有这些问题都是有意义的 —— 其中有许多过于容易, 另一些则显得过分地人为造作 —— 但其中有一些问题是非常自然的, 而当人们试图去解决它们时, 一开始又时常是极难解决的. 这时常是一个信号：碰上了一个数学家称为 "深刻" 的问题. 本节下面的部分就看一个这样的问题.

群 G 称为有限生成的, 如果 G 有一个元素的有限集合 $\{x_1,x_2,\cdots,x_k\}$, 使得群的其余的元素都可以写成它们的乘积. 例如群 $\mathrm{SL}_2(\mathbf{Z})$ 的元素就是有整数元的 2×2 矩阵 $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, 其中 $ad-bc=1$. 这个群就是一个有限生成的, 证明它的所有元素都可以用 4 个矩阵 $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ 和 $\begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$ 通过矩阵乘积来生成, 这是一个好习题 (关于矩阵的讨论见 [I.3 §3.2]. 第一步是证明 $\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}=\begin{pmatrix} 1 & m+n \\ 0 & 1 \end{pmatrix}$).

现在考虑第二个性质. 若 x 是群 G 的一个元, 则说 x 是有限阶的, 如果存在 x 的一个幂, 恰好等于恒等元. 这个最小的幂就称为 x 的阶. 例如, 在非零整数 mod 7 的乘法群中, 恒等元就是 1, 元素 4 的阶是 3, 因为 $4^1=4$, $4^2=16\equiv 2 \bmod 7$, $4^3=64\equiv 1 \bmod 7$. 至于 3, 它的前 6 个幂是 3, 2, 6, 4, 5, 1, 所以它的阶是 6. 有一些群有一个特殊的性质, 即存在一个 [正] 整数 n, 使得对于群的一切元素 x , x^n 都是恒等元 —— 或者用一个等价的说法, 即所有元素的阶都是 n 的一个因子. 对于这种群, 我们能说些什么？

现在先看所有的元素都以 2 为阶的情况. 用 e 表示恒等元, 我们的假设就是,

对于每一个元素 $a, a^2 = e$. 如果用逆元 a^{-1} 去乘上式双方, 就得出 $a = a^{-1}$. 反向的蕴含也容易证明, 所以这种群就是所有元都等于自己的逆元的群 G.

现在令 a , b 是 G 的两个元. 对于任意群的任意两个元 a, b, 总有恒等式 $(ab)^{-1} = b^{-1}a^{-1}$(这仅仅是因为 $abb^{-1}a^{-1} = aa^{-1} = e$), 而对于特殊的群 G, 则还可以由此导出 $ab = ba$. 就是说, G 自动地是阿贝尔群.

我们已经看到一个一般性质: G 的每个元平方以后均得恒等元, 蕴含了另一个一般性质: G 为阿贝尔群. 现在再加上一个条件: G 为有限生成群, 而令 $x_1, x_2, \cdots, x_k$ 为生成元的最小集合, 即是说, 群 G 的每一个元素都可以从 $x_1, x_2, \cdots, x_k$ 构造出来, 而且这些 x_i 一个也不能少. 因为群 G 是阿贝尔群, 而每一个元素又都等于自己的逆元, 就可以重新排列这些 x_i 的次序, 把这个元素化为标准形式, 即各个 x_i 只出现一次, 而且依下标的次序排列. 例如看乘积 $x_4x_3x_1x_4x_4x_1x_3x_1x_5$. 因为群 G 是阿贝尔群, 这个乘积就等于 $x_1x_1x_1x_3x_3x_4x_4x_4x_5$. 又因为每个元都等于自己的逆元, 所以这个元就等于 $x_1x_4x_5$. 这就是标准形式.

这就证明了群 G 最多只有 2^k 个元素, 这是因为对于每一个 x_i 都有两种选择, 即或者包含或者不包含在标准形式中. 特别是 "群 G 为有限生成的" 以及 "群 G 的每一个非恒等元均等于自己的逆元" 这两个性质就蕴含了第三个性质: "群 G 为有限群". 还可以很容易地证明, 若两个元素的标准形式不同, 则它们本身自然也不同, 所以, 群 G 确实恰好有 2^k 个元素 (这里 k 是最小生成元组的大小).

现在我们要问, 如果使得对于一切元 x 都会有 $x^n = e$ 的这个幂指数 $n > 2$, 会发生什么? 即是说, 如果群 G 是有限生成的, 而且对一切元 x 都有 $x^n = e$, 群 G 是否必为有限群? 这是一个难得多的问题, 最早是由本塞德[VI.60] 提出的. 本塞德本人证明了若 $n = 3$, 则群 G 必为有限群, 但是直到 1968 年前一直没有大的进展, 1968 年 Adian 和 Novikov 得到了一个值得注意的结果, 即若 $n \geqslant 4381$, 群 G 不一定是有限的. 当然, 在 3 和 4381 之间还有很大的间隙, 在这个间隙上建一座桥的工作进展很缓慢. 只是到了 1992 年, 才由 Ivanov 改进到 $n \geqslant 13$. 想要体会一下本塞德问题有多难, 只需看一下以下的情况就明白了: 甚至两生成元的群, 若每个元的五次幂均为恒等元, 此群是否有限都还未知.

8. 利用不完全严格的论证

如果一个数学命题的证明符合严格性的高标准 (有这样一个高标准正是数学这门学科的特征), 这个命题就算是得以确立. 然而, 不严格的论证在数学里也有重要的作用. 举例来说, 如果希望把一个数学命题用于另一个领域, 比方说是工程或物理学, 则命题是否为真实的就比命题是否已经证明了更加重要.

然而, 这就导致了一个明显的问题, 如果还没有证明一个命题, 那么, 相信这个

命题为真有什么基础呢？事实上有好几种不严格的说明正当性的方法[①]，我们来看其中的几个.

8.1 有条件的结果

前面已经提到，黎曼假设是数学里最著名的未解决问题. 为什么认为它那么重要? 比方说, 为什么它比孪生素数猜想更重要? 而后一个猜想同样是关于素数序列的性态的.

主要的但不是唯一的理由在于黎曼假设及其推广有为数巨大的推论. 用宽泛的语言来说, 黎曼假设告诉我们：说素数序列中出现了一定程度的“随机性”并不会产生误导：素数在许多方面性态很像适当选择的随机的整数集合.

如果素数以随机的方式行事, 人们可能会以为这将使得素数更难以分析了, 但是, 事实上随机性是有好处的. 举例说, 正是因为有随机性, 我们才深信, 在伦敦, 在 20 世纪的每一天都至少有一个女孩出生. 如果婴儿的性别不那么随机, 我就不会那么肯定了, 说不定婴儿的出生有某种奇特的模式, 例如女孩出生在星期一到星期四, 男孩出生在星期五到星期日. 类似地, 如果知道素数的形态像一个随机序列, 则对于素数在长时期的平均性态就会知道许多知识. 黎曼假设及其推广用精确的方式陈述了这样一个思想, 即素数, 还有在数论理出现的其他重要序列, 都会“随机地行事”. 这才是有那么多推论的原因所在. 有大量的论文, 其中都有一些定理, 是在假设黎曼假设的某种形式已经得证的条件下才成立的. 所以, 如果证明了黎曼假设, 就改变了所有这些定理的状态：从在某种条件下成立变为得到了完全的证明.

如果一个定理依赖于黎曼假设, 我们怎样去看待这个定理？可以简单地说, 现在证明了黎曼假设蕴含这个定理, 然后对这个定理就置之不理了. 但是, 绝大多数数学家会采取另一种态度. 他们相信黎曼假设, 相信终有一日黎曼假设会得到证明. 所以他们也会相信其所有推论, 哪怕他们也认为那些已经无条件地得到证明的结果才更靠得住.

还可以在理论计算机科学中举一个大家都很相信并且用它来作为进一步研究的基础的例子. 我们在 §6.4 中提到, 计算机科学的主要目标之一就是要确定计算机能够多快就完成一项工作. 这个目标分成了两部分：一是找出以尽可能少步数完成任务的算法; 二是证明 [完成这个任务的] 每一种算法必定至少需要一定数量的步数. 第二个工作是难得出了名的, 最好的已知结果远远弱于大家信以为真的结果.

有一类计算问题, 称为 NP 完全问题, 这一类问题具有同等的难度. 就是说如果

---

① 原文用的是 justification 一词. 数学书上时有用此词代替“证明”一词的, 因为本节的目的正是想要说明不必仅限于符合严格性的高标准, 所以用了比较冗长的文字“说明正当性的方法”来翻译 justification 一词. 下同. —— 中译本注

其中有一个问题有有效率的算法[1], 则此算法可以转化为对所有其他这一类问题的有效率算法. 然而, 在很大程度上正是由于这个原因, 几乎普遍都相信这一类问题中没有一个具有有效率的算法, 或者, 通常就把这个信念说成是: “P 不等于 NP”. 所以, 如果想证明某一个问题不存在快速算法, 只需要证明这个问题和某个已知为 NP 完全的问题至少一样难. 这还不算是一个严格证明, 但是对其正当性是一个很有说服力的说明, 因为绝大多数数学家都相信 P 不等于 NP(关于这个问题, *计算复杂性*[IV.20] 中有更多的讨论).

有一些研究领域依赖于好几个假设而不只是依赖于一个假设. 这个领域的研究者好比是发现了一处数学美景, 他们急不可耐地想把地图画出来, 尽管还有许多他们并不了解的事情. 这时常是一个很好的研究策略, 就是从将来找到严格证明的前景来看也是. 一个猜想, 并不是空洞大胆地随便去猜, 它的内涵要丰富得多: 一个猜想, 要想被接受为重要的猜想, 要经历多种检验. 例如, 它有没有已经知道为真的推论? 有没有一些人们能够证明的特例? 如果它是真的, 是否有助于解决其他问题? 是否得到了数值证据的支持? 如果它是不成立的, 是否会给出容易反驳的大胆的精确命题? 需要极大的洞察力和艰苦工作才能得出一个能够通过这些检验的猜想, 但是如果成功了, 得到的就不仅是一个孤立的命题, 而是一个与其他命题有多种联系的命题. 这就增加了它得到证明的机会, 大大增加一个命题的证明导致其他命题也得到证明的机会. 一个好的猜想, 甚至其反例也能揭示许多东西, 如果这个猜想与许多其他命题有关, 它的效果将会渗透到整个领域之中.

一个充满猜想性命题的领域是*代数数理论*[IV.1], 特别是朗兰茨纲领, 它是由朗兰茨 (Robert Langlands) 提出的许多猜想的整体, 把数论和表示理论连接了起来 (这一点将在*表示理论*[IV.9 §6] 里讨论). 此外, 它还把许多猜想和结果都推广了, 统一了, 解释了. 例如, 其中就有志村–谷山–韦伊 (Shimura-Taniyama-Weil) 猜想, 而这个猜想对于怀尔斯证明*费马大定理*[V.10] 起了中心作用, 而这个猜想还只是朗兰茨纲领的一个小部分. 朗兰茨纲领极好地通过了一个好猜想需要通过的检验, 多年来指导了许多数学家的研究工作.

另一个具有类似本性的领域是一个称为*镜面对称*[IV.16] 的领域. 它是一种*对偶性*[III.19], 把来自*代数几何*[IV.4] 以及*弦论*[IV.17 §2] 的一个称为 *Calabi-Yau 流形*[III.6] 的对象和其他对偶的流形连接起来. 正如某些微分方程, 如果考虑相关函数的*傅里叶变换*[III.27] 就比较容易求解一样, 在弦论里出现的一些计算, 如果不是变换为对偶的, 即 “镜面” 的情况, 就无法进行计算. 这种变换至今还没有被严格地说明其合理性, 但是这个过程已经给出了一些极复杂的几乎没有人会猜想到的公式. Maxim Kontsevich 提出了一个精确的猜想, 可以解释镜面对称的明显的成功.

[1] 何谓有效率的算法, 见 [IV.20 §2].—— 中译本注

8.2 数值证据

哥德巴赫猜想[V.27]指出, 每一个大于或等于 4 的偶数都是两个素数之和, 如果有人要想用今天的数学工具证明它, 即令他准备接受黎曼猜想, 似乎也不敢有此奢望. 然而人们又都以为这个命题肯定为真.

相信哥德巴赫猜想有两个主要理由. 第一个理由已经遇见过: 如果素数真是"随机分布的", 则可以期望它为真. 这是因为若 n 是一个大偶数, 则有许多方法写出 $n = a + b$, 而有足够多的素数使得人们敢于期望 a 和 b 有时会同时成为素数.

这样的论证还留下一个漏洞, 即有可能对于太大的 n, 我们没有交上好运, 使得当 a 为素数时, $n - a$ 必为合数. 数值证据在这里就出来了. 现在已经核验过, 每一个直到 10^{14} 为止的偶数都能写为两个素数之和, 所以当 n 更大时, 极不可能偏偏倒霉, "恰好" 碰上这么一个反例.

这或许是一个太粗糙的论据, 但是有一个办法使它更为可信. 如果能使素数为随机分布这个思想更加精确, 就可以陈述哥德巴赫猜想的一个更强的版本, 就是不但指出每个偶数都可以写成两个素数之和, 而且还粗略地说有多少种写法. 例如, 如果 a 和 $n - a$ 都是素数, 则其中没有一个可以是 3 的倍数 (除非它自己就是 3). 若 n 是 3 的倍数, 则这只是说 a 不能是 3 的倍数, 但是若 n 可以写成 $3m + 1$, 则 a 不能也是 $3k + 1$ 的形式, 否则 $n - a$ 就会是 3 的倍数了. 这样, 在某种意义下, 若 n 是 3 的倍数, 则把 n 写为两个素数之和要容易 "两倍". 考虑到这些信息就可以估计出, "应该" 有几种方式把 n 写成两个素数之和, 结果是每一个偶数 n 都应该有多种方法写为两个素数之和. 此外, 对于 "有多少个" 的预测与数值证据可以密切配合, 就是说对于小的 n 可以在计算机上检验这些预测是否正确. 这就使得数值证据更为可信, 因为它不只是对于哥德巴赫猜想的证据, 而且还是对于更加一般的原理的证据, 因此引导我们更加相信它.

这是一个一般现象的例证: 由某一个猜想得到的预测更精确, 则它后来被数值证据证实时, 就会给人留下更深的印象. 当然, 不只对于数学是如此, 对于更一般的科学也是如此.

8.3 "不合法" 的计算

在 §6.3 中, 关于一个 n 步的自避游动的起点与终点的平均距离, 我们说 "关于它几乎是一无所知". 对于这样一个说法, 理论物理学家会强烈地不同意. 相反地, 他们会告诉您, 一个典型的 n 步的自避游动的起点与终点的平均距离是在 $n^{3/4}$ 左右. 这种明显的不一致可以用以下的事实来解释, 物理学家们有许多不严格的方法. 尽管几乎都没有严格证明过, 但是, 如果小心使用, 似乎能给出正确的结果. 物理学家们用自己的方法, 能够在一些领域里确立一些命题, 而这些命题远非数学家所能够证明. 这些结果对数学家是很有吸引力的, 部分地是因为如果把物理学家的

结果看成数学的猜想, 则按照前面所讲的标准, 其中有许多都是极出色的猜想: 它们是深刻的, 完全不可能在事前猜出来, 被广泛认为是真实的, 有数值证据支持, 等等. 其吸引力的另一个理由在于, 如果下力气去搞出严格的支撑, 这种努力在纯粹数学领域里常会带来显著的进步.

为了对物理学家的不严格计算是什么样的东西得到一点印象, 下面对 Pierre-Gilles de Gennes 在物理学家的某些结果后面的著名论证作一个粗糙的描述 (这些结果也不妨称为一种预测, 如果您喜欢这样说的话). 在统计物理中有一个模型, 称为 n 向量模型, 它与临界现象的概率模型[IV.25] 中的伊辛 (Ising) 模型和 Potts 模型有密切的关系. 在 $\mathbf{Z}^d$ 的每一点上都给定一个 $\mathbf{R}^n$ 单位向量. 这就给出了一个单位向量的随机构形, 我们对它赋予一个 "能量", 这个能量随着相邻向量间的角度而增加. De Gennes 找到了一个方法把自避游动问题加以变换, 使得可以把它看成 $n=0$ 时的 n 向量模型. 但是 0 向量模型是没有意义的, 因为在 $\mathbf{R}^0$ 中并没有单位向量. 然而 De Gennes 仍找到了与 n 向量模型相关的参数, 并且证明, 当 n 趋于零时, 就会得到与自避游动相关的参数. 他进而在 n 向量模型中选取其他参数来导出关于自避游动的信息, 例如所希望的起点与终点的平均距离.

对于纯粹数学家, 这种途径有下面的令人十分烦恼的事情. 当 $n=0$ 时, 在 n 向量模型中的公式是没有意义的, 所以人们就把它们看作是当 $n\to 0$ 时的极限. 但在 n 向量模型中的 n 非常清楚是一个正整数, 那正整数怎么能够趋于 0 呢? 是不是还有办法对于更一般的不一定是正整数的 n 也来定义 n 向量模型呢? 说不定, 但是谁也没有做到过. 可是 De Gennes 的论据, 还有其他类似的论据, 引导到非常精确的预测, 而且与数值证据十分符合. 这里面必定有好理由, 虽然谁也不知道是什么理由.

本节所举的例子只是很少几个例证, 说明数学怎样因不严格的论证而得到丰富. 这些论据使我们能够更深入到数学的未知领域, 开辟了整个研究领域, 研究那些本来会从眼皮子下面溜走的现象. 话说到这个地步, 人们会怀疑严格性是否重要: 既然由不严格的论据所确立的结果很清楚为真, 这不就足够好了吗? 确实有这样的事: 有例子表明, 确实有不严格的方法 "建立起来的" 命题后来被证实是不对的, 可是关注严格性的最重要的理由是: 由严格的证明所得到的理解, 比起由不严格方法提供的理解, 要更加深刻. 描述这里的情况最好的方法, 也许是说, 这两种不同风格的论证, 过去是彼此深刻的互相得益, 无疑今后还会是这样.

9. 寻求显式的证明和算法

方程 $x^5-x-13=0$ 显然有一个解. 说到底, 令 $f(x)=x^5-x-13$, 有 $f(1)=-13, f(2)=17$. 所以, 在 1 和 2 之间必有一个 x 使 $f(x)=0$.

这是纯粹存在论证的一个例子, 这种论证告诉您有什么东西存在 (在此例中,

是一个方程的解), 但是没有说怎样去求它. 如果方程是 $x^2 - x - 13 = 0$, 就可以用一种全然不同的论证. 二次方程求根的公式告诉我们, 恰好有两个解, 它甚至告诉我们解是什么 (它们是 $(1+\sqrt{53})/2$ 和 $(1-\sqrt{53})/2$). 但是对于五次方程就没有类似的公式 (见*五次方程的不可解性*[V.21]).

这两种论证表现了数学的基本的两分法. 如果要证明一个数学对象的存在, 有时可以显式地证明, 就是实实在在地描述那个对象; 也可以间接地去证明, 就是证明如果它不存在就会引起矛盾.

介于其间还有种种可能性, 形成一个谱. 如所说明过的, 上一个论证只是说明, 在 1 与 2 之间, 方程 $x^5-x-13=0$ 有一个解, 但它也建议了一种方法来计算这个解, 精确到如您所需. 例如, 如果需要精确到两位小数, 可以取一串数: $1, 1.01, 1.02, \cdots, 1.99, 2$, 然后在每一点估算 f 之值. 就会发现, $f(1.71)$ 近似为 -0.0889, 而 $f(1.72)$ 近似为 0.3337, 所以其间必有一个解 (计算表明, 此解更靠近 1.71). 事实上还有更好的方法, 例如*牛顿方法*[II.4 §2.3] 去逼近一个解. 对于许多目的, 一个漂亮的解的公式不如计算或逼近这个解的方法更重要 (关于这一点的进一步讨论, 可见*数值分析*[IV.21 §1]). 而如果有了一个方法, 它是否有用, 还要看它运行快不快.

这样, 在谱的一端有简单的定义一个熟悉对象的公式, 它还可以容易地用来求出这个对象, 而在谱的另一端, 则有能够确立对象的存在性但不给出进一步的信息的证明, 介乎其间的还有能够用以找出对象的算法, 这些算法执行起来越快, 其用处就越大.

和关于严格性的问题一样, 如果一切其他条件都相同, 则严格的论证优于不严格的论证. 现在, [在直接和间接论证的问题上, 也是] 即令已经知道有间接存在证明, 找到一个显式的有算法的论证仍然是值得的, 其理由也是类似的: 寻求显式论证所花的力气时常导致新的数学洞察 (不那么明显的是: 寻找间接论证的努力, 有时也会带来新的洞察).

纯粹存在证明的最著名的例子之一是关于*超越数*[III.41] 的. 超越数就是那些不可能是任意整数系数的多项式方程之根的实数. 有这种数存在的第一个证明是*刘维尔*[VI.39] 在 1844 年给出的. 他证明了有一个条件足以保证一个数是超越的, 而且证明了构造出满足这种条件的数也是容易的 (见*刘维尔定理*和 *罗特定理*[V.22]). 后来, 各种重要的数如 e, π 都被证明是超越数, 但是这些证明都很难. 甚至到了现在, 仍有许多数几乎肯定是超越数, 但是就是证明不出来 (这方面更多的信息, 可见*无理数和超越数*[III.41]).

以上所说的证明全都是直接显式的. 然后, 到了 1873 年*康托*[VI.54] 利用了他的*可数性理论*[III.11] 给出了超越数存在的完全不同的证明. 他证明了代数数成一可数集合, 而实数构成一个不可数集合. 因为可数集合远小于不可数集合, 这表明几乎每一个实数 (虽然不一定是几乎每一个您真正见到的实数) 都是超越数.

就这个例子而言, 两种论证的每一种都告诉了我们另一种论证所没有告诉我们的事. 康托的证明告诉了我们确有超越数存在, 但却一个例子也没有给我们 (严格说来, 这也不是真的: 可以指定一种方法把代数数排成一个单子, 然后对这个单子应用康托著名的对角线论证法, 就可以找到一个超越数, 然而这样找出来的超越数基本上没有任何含义). 刘维尔的证明在一个方面要好得多, 因为它给了我们一个方法, 用直截了当的定义来构造出几个超越数. 然而, 如果只知道刘维尔的那种直接论证以及 e, π 为超越数的证明, 就可能得到一个印象, 即超越数是一种很特殊的数. 有一种洞察在这些论证里完全见不到, 但在康托的证明里面出现了, 即典型的实数是超越数.

在 20 世纪的大部分时间里, 高度抽象的间接证明大行其道, 但是在最近的年代, 特别是因为有计算机的发明, 态度起了变化 (这当然是就整个数学界的一般情况的说法, 而不是指个别的数学家). 近来, 得到更多注意的是: 一个证明是否为显式的, 如果是, 又是否能导出有效率的算法.

无需说明, 算法本身就是有趣的, 这还不尽是由于它们给予数学证明的视角. 作为本节的结束, 我们简短地描述一个特别有趣的算法, 它是好几位作者近几年间发展起来的, 给出了一种计算高维凸体体积的方法.

一个图形 $K[\mathbf{R}^n]$ 称为凸体, 是指在 K 内任取两点 x 与 y, 则连接 x 与 y 的直线段全在 K 内. 例如, 正方形和三角形都是凸的, 而五角星就不是. 这个概念可以直接推广到 n 维情况, n 是任意正整数. 面积和体积的概念也能这样推广.

现在设在以下意义上指定了一个 n 维的凸体 K, 即设有了一个运行很快的计算机程序, 它能告诉我们每一个点 $(x_1, \cdots, x_n)$ 是否属于 K. 怎样来估计 K 的体积呢? 对于像这样的问题, 最有力的方法之一是统计方法: 随机地取一点, 看它是否属于 K, 把对 K 的体积的估计建立在这个点落入 K 中的频度上. 例如, 想估计 π, 就取一个半径为 1 的圆, 把它放在一个边长为 2 的正方形里面, 然后从这个正方形里随机地取许多点. 每一个点属于此圆的概率都是 $\pi/4$(即圆的面积 π 与正方形的面积 4 之比), 所以把落入圆内的点占点的总数的比乘以 4, 就得到 π 的 1 估计.

这个途径对于很低的维数是很容易起作用的, 但是当维数很高时, 却会遇到很大的困难. 例如设我们想用这个方法估计 n 维球的体积. 把这个球放在一个 n 维立方体里面, 也去看这个点落入球内的频度. 然而, n 维球的体积占 n 维立方体体积的比却是指数的小, 这就是说, 在球内找到一个点前, 先要投的点的数目是指数的大. 所以这个方法毫无希望地变得不切实用.

然而并不是一切都完了, 因为还有一个计策可以绕过这个困难. 可以定义一个凸体的序列 $K_0, K_1, \cdots, K_m$, 使每一个凸体都包含于下一个凸体内, 而从想要计算其体积的凸体开始, [即想计算 K_0 的体积], 而终于一个立方体, [即 K_m 是一个立方体], 并且使得 K_i 的体积至少是 K_{i+1} 的体积的一半. 于是对每一个 i, 都要估计一

下 K_{i-1} 与 K_i 的体积之比. 这些比的乘积就是 K_0 与 K_m 的体积比. 但是 K_m(立方体) 的体积是知道的, 所以就得到 K_0 的体积.

怎样来估计 K_{i-1} 与 K_i 的体积之比呢? 只需简单地随机取 K_i 之点, 并且看有多少落入 K_{i-1} 中. 然而就是在这里, 问题的微妙之处出现了: 怎样从知之不多的凸体里随机取点呢? 在 n 维立方体里随机取点是容易的, 只需要独立地选取 n 个随机数 $x_1, \cdots, x_n$, 而每一个 x_i 都在 -1 和 $+1$ 之间. 但是对于一个凸体这就非常不容易了.

有一个奇妙的聪明办法来回避这个问题. 这就是小心地设计一个随机游动, 从凸体内的一点开始, 而在每一步, 移动到的点可以从几个不多的可能性中随机选择. 随着随机的游动步数越多, 对于这点所到达的地方所知就越少. 如果这个游动是适当定义的, 可以证明, 在不多几步以后, 点的位置就是纯粹随机的了. 然而, 证明完全不容易 (在条目高维几何学及其概率类比[IV.26 §6] 中还有更详细的讨论).

关于算法及其数学的重要性的讨论, 请参看算法[II.4]、计算数论[IV.3]、计算复杂性[IV.20] 以及算法设计的数学[VII.5].

10. 您在数学论文里会找到什么

数学论文有着非常独特的体裁, 这是在 20 世纪初建立起来的. 本文的最末的这一节就想对数学家实际写出来的东西作一个描述.

一篇典型的数学论文通常都是形式的和非形式的写作的混合物. 在理想情况下 (但绝非总是如此), 作者要写一个可读的引言, 告诉读者他能在本文余下的部分里读到什么. 如果文章分成几个部分, 绝大多数文章, 除非太短都会分成几个部分, 则若每一部分都以下面的论证的非形式的大纲开始, 那对于读者就会很有帮助. 但是文章的主要实质部分应该是比较形式、比较详细的, 使得如果读者打算花上充分的力气, 他就能说服自己: 这篇文章是正确的.

一篇典型的论文的目的是建立起一些数学命题, 有时目的仅在于此. 例如, 论文的价值就是它证明了一个 20 年没有解决的猜想. 有时, 建立这些数学命题是为了一个更广泛的目标, 例如解释一个人们理解不够的数学现象. 但是, 不管是哪一种, 数学命题都是数学的主要价值所在.

命题中最重要的通常称为定理 (theorem), 但是也有些命题就称为命题 (propositon), 还有时叫做引理 (lemma)、推论 (或者叫系)(corollary). 这些种类的命题很难作清楚的划分, 但是它们的字面意思也就说明了怎样区分. 定理就是您认为是具有内在的兴趣的命题, 它可以从一篇论文里抽出来, 例如用来对朋友们讲, 在讨论班上作报告. 成为论文的主要目标的命题通常就叫定理. 一个命题其实也就是一个定理, 但是它们时常有点令人 “厌烦”. 论文里面要去证明令人厌烦的结果, 听起来有些奇怪, 但是它们可能是重要而且有用的. 它们令人厌烦, 是由于它们怎么也使人

惊奇不起来. 它们就是那些我们需要、也希望其为真、证明起来也没有困难的定理.

下面是一个简单的例子, 是一个可能更愿意称之为命题的定理. 二元运算 [I.2 §2.4]“$*$” 的结合律指出：$x*(y*z)=(x*y)*z$. 我们时常把这个定律非正式地说成是 “括号不起作用”. 然而, 尽管它告诉我们, 直接写 $x*y*z$ 也不会引起歧义, 可是, 例如说 $a*b*c*d*e$ 也不会引起歧义, 就不那么显而易见了. 我们怎么知道仅仅因为在三个对象的情况下, 括号的位置没有影响, 则在多于三个对象的情况, 括号也不起作用?

许多学数学的大学生, 心情愉快地读完了大学, 却没有注意到这还是一个问题. 似乎结合律就表示括号不起作用. 他们基本上是对的, 虽然并不完全显然, 但是证明这一点不会给人带来惊喜, 而且结果是很容易证明的. 因为我们时常会需要这个简单的结果, 又很难称它为定理, 把它称为一个命题也还是适合的. 为了对如何证明它有一点感觉, 您可以去证明一下, 结合律蕴含了以下等式：

$$(a*((b*c)*d))*e=a*(b*((c*d)*e)).$$

然后, 您就可以试着推广正在做的事.

当证明一个定理时, 证明时常过长也过于复杂. 这时, 如果希望有人愿意读下去, 就需要使证明尽可能清晰. 做这件事最好莫过于建立一些子目标, 其形式就是位于假设和我们想得到的结论之间的一些中介的命题. 这些命题时常就称为引理. 举一个例子：假设想对 $\sqrt{2}$ 是一个无理数的标准证明给出一个非常详细的表述. 有一个需要的事实就是：每一个分数 p/q 都等于一个分子分母不同时为偶数的分数, 即可将 p/q 写成 r/s, 其中 r 和 s 不能全是偶数, 而这个事实也需要证明. 为清楚起见, 您会决定把这个证明从主要的证明中分离出来, 并称之为一个引理. 这样, 就把自己的工作分成了两个分开的工作：一是证明引理, 二是用这个引理去证明主要的定理. 可以把这个做法与写计算机程序平行对照起来：当写一个复杂的程序的时候, 一个好办法是把主要任务分成一些子任务, 并且各写一个小程序, 把这些小程序当成“黑盒子”, 以便在用得着的时候让程序的其他部分去访问它们.

有些引理很难证明, 而且在不同的背景下也用得着, 所以最重要的引理比那些不甚重要的定理可能更重要. 然而有一个一般的规则, 如果证明一个结果的主要理由在于把它用作证明其他结果的踏脚石, 那就把这个结果称为引理.

如果一个数学命题可以容易地从另一个命题导出, 就称它为另一个命题的系 (或者直接就说是其推论), 有时, 一个主要定理后面接着几个系, 借以说明这个定理的力量. 有时, 主要定理也叫做系, 因为证明的所有工作都是为了证明一个不同的、不那么简练有力的结果, 而主要定理可以由它很容易地得出来. 如果发生了这种情况, 作者应会说明, 这个系是论文的主要结果, 而其他作者则会称之为定理.

一个数学命题是通过证明来确立的. 数学的一个最值得注意的特点就在于可

以有证明, 例如, 一个由欧几里得[VI.2] 在大约两千多年前发明的论证在今天仍然被接受为完全有说服力的证明. 然而, 一直到 19 世纪末和 20 世纪初, 这个现象才为人恰当地理解, 就是直到数学语言被形式化以后 (所谓形式化是什么意思, 请见数学的语言和语法[I.2], 特别是其中的 §4). 到那时他才可能把证明的概念弄明确. 从逻辑学家的观点来看, 所谓证明就是一连串的数学命题, 每一句都用形式语言写成, 而且具有以下的性质: 最前几个命题是初始的假设, 或称前提; 这一串中的其余命题根据逻辑的规则, 从它们前面的命题得出, 这些逻辑规则又如此简单, 所以这些推导都清楚地是有效的 (下面的例子就是这些规则之一例, 从中可以看出它们确实是无可争议的: "若 $P \wedge Q$ 为真, 则 P 为真", 这里的 "$\wedge$" 就是 "与" 的逻辑记号); 这一串命题的最后一个就是想要证明的命题.

对于实际出现在一篇规范化的数学论文, 写在 "证明" 这个标题下的东西, 只是上述关于证明的思想的理想化. 这是因为一个纯粹形式化的证明将是冗长而几乎无法卒读的. 尽管如此, 论证在原则上可以形式化这个事实, 为数学大厦提供了非常有价值的支撑, 因为它给出了解决争论的途径. 如果一位数学家给出了一个奇怪的没有说服力的论证, 要看它是否正确, 最好的方法就是请他或她作出更加形式化、更加详细的解释. 这样做, 要么会暴露出错误, 要么会使得这个论证更加清楚.

数学论文的另一个非常重要的成分是定义. 这本书里面充满了定义, 特别是在第III部分. 有一些定义的给出只是为了使得讲起话来更简明. 举例来说, 如果要证明一个关于三角形的定理, 而且总是需要用到从一个顶点到对边的距离, 这就麻烦了, 因为总需要说 "从 A, B, C 分别到 BC, CA, AB 的距离", 这样, 就不如选择一个词 "高", 并且写道: "给定三角形的一个顶点, 定义其高为从一个顶点到它的对边的距离". 如果考虑的三角形是钝角三角形, 就得小心一点, 写道: "给定三角形 ABC 的顶点 A, 定义其高为由 A 到通过 B, C 两点的唯一直线的距离". 从此以后, 就可以使用 "高" 这个词, 而不必说上那一大段话, 行文就简洁多了. 像这样的定义不过是为简便而给定的定义, 只要需要, 总是相当清楚该做什么, 而我们也就这么做了. 但是, 真正有趣的定义是不那么显然, 而是一旦有了它, 就会用新的方式来思考的那种定义. 一个很好的例子就是函数导数的定义. 如果您不知道它, 对于如何求实的函数 $f(x) = 2x^3 - 3x^2 - 6x + 1$ 达到最小的正的 x, 您的思想就是一片空白. 如果您真的知道了它, 这个问题就成了一个简单的习题. 这可能有点夸张, 因为您还得知道, 这个最小值会出现在 0 处, 或者出现在导数为 0 处, 您还得知道如何微分 $f(x)$, 但这些都是简单的事实 —— 说是定理, 不如说是命题 —— 真正的突破是在概念本身.

像这样的定义有许多例子. 但是有趣的是, 在数学的某些分支里面, 它们比在其他分支里面更加常见. 有些数学家会告诉您, 他们的研究的主要目的就在于找出正确的定义. 有了这些定义, 他们的整个领域就被照亮了. 确实, 他们必须要去写证

明, 但是, 如果定义正是他们所寻找的, 证明时常会是相当直截了当的. 是的, 有他们能用这些定义来解决的问题, 但是, 就和上面的极小化问题一样, 这些问题对于整个理论并不是中心, 说这些数学家是在展示他们的定义的力量更恰当些. 对于另外一些数学家, 定义的主要目的在于证明定理, 但是, 甚至这些非常的以定理的证明为导向的数学家时而也会发现, 一个好的定义对于增强解决问题的本领起了重大的作用.

这就把我们引导到 [怎样看待] 数学问题. 一篇数学论文的主要目的通常都是证明定理. 但是, 读文章的主要理由之一却是为了推进自己的研究. 所以, 如果一个定理是用了一种可以用于其他背景的技巧, 那么这篇文章是会受欢迎的. 如果一篇文章里面包含了好的未解决的问题, 它也会受到很大的欢迎. 作为一个例证, 我们来看一个绝大多数数学家都不会认真对待的问题, 借以从中看到这个问题缺少了些什么.

一个数称为回文数, 如果它的十进表达式是回文的形式[①]: 22, 131 和 548 845 都是回文数的例子. 当然, 131 是有趣的, 因为它是一个素数. 让我们试着来找更多的素回文数. 一位的素数当然都是回文的, 而二位回文数必以 11 为因子, 所以, 只有 11 本身是素数. 这样, 我们很快就到了三位数. 这里有几个素回文数的例子: 101, 131, 151, 191, 313, 353, 373, 383, 727, 757, 787, 797, 919 和 929. 不难看到, 所有偶数位回文数都以 11 为因子. 但是, 素回文数并未止于 929—— 例如, 10301 就是下一个最小的素回文数.

现在, 任何一位稍有一点点好奇心的人都会问: 是否有无限多个素回文数? 结果是, 这居然是一个未解决的问题. 人们相信是有无限多个素回文数 (这是基于素数应该是充分随机的, 而奇数位的回文数也看不出有特别的理由一定就有因子), 但是谁也不知道如何去证明它.

这个问题有一个很大的优点, 就是它很容易懂, 这使它很吸引人, 但*费马大定理*[V.10] 和*哥德巴赫猜想*[V.27] 不也正是由于很容易懂而吸引人吗? 但是这个素回文数的问题并不像后两个问题那样, 不能成为中心的问题. 绝大多数的数学家会把它放进 "休闲数学" 或者 "数学游戏" 这样的智慧宝盒里去, 然后就忘得一干二净.

这种抛弃的态度的理由何在呢? 难道素数的研究不是数学的中心对象吗? 确实是的, 但是回文数却不是, 其所以不是的主要理由在于 "回文数" 的定义极端地不自然. 如果知道了一个数是回文数, 则与其说是知道了这个数的特性, 不如说知道的是表示这个数的方式的特性, 而由于历史的原因, 我们恰好是采用了这个方式. 特别是, 具有回文数形式依赖于我们选取了以 10 作为记数的基底. 设若以 3 位记

① 所谓回文就是正读和反读都相同的文字, 这只是一种文字游戏, 所以在文学上并没有什么价值.——中译本注

数法的基底, 131 这个数将写成 11212, 倒过来写就不一样了.

这个说法虽然有一定的说服力, 却不是完整的解释, 因为有可能某些有趣的性质正是牵涉到 10 的, 至少是可能有有趣的性质与人为地选取某个特定的数有关. 下面再举一个例子, 形如 2^n-1 的素数是否有无穷多个, 这个问题被认为是有趣的, 虽然其中使用了一个特别的数 2, 选用 2 是有正当理由的. [因为若取 $a>2$, 则 a^n-1 恒有因子 $a-1$(它是一个大于 1 的正整数), 所以, 除非 $n=1$, a^n-1 一定不是素数. 因此, 形如 a^n-1 的素数是否有无穷多个], 这个问题的答案一定为否. 此外, 形如 2^n-1 的数还有许多性质, 使它们更可能是素数 (关于这一点的解释可见**计算数论**[IV.3]). 但是, 即令把 10 换成一个 "更自然的" 数 2, 并且来看那些回文数写成二进制后怎样, 那也还得不到一个会被看成严肃的研究主题的性质. 设给定一个正整数 n, 定义 $r(n)$ 为其颠倒数, 就是先把它写成二进制, 再颠倒次序来写, 这样得到的数. 这时, 一个二进制意义下的回文数, 就是使得 $n=r(n)$ 的数 n. 但是, 函数 $r(n)$ 是非常奇特而且 "非数学" 的. 举例来说, 从 1 到 20 这些数的颠倒数依次是: 1, 1, 3, 1, 5, 3, 7, 1, 9, 5, 13, 3, 11, 7, 15, 1, 17, 9, 25, 还有 5, 这给出了一个看不出任何模式的序列. 实际上, 当我们计算这个序列时, 就会看到它比初看起来还更加是人为的. 人们可能会想, 颠倒数的颠倒数就是这个数本身, 但是不然. 例如取数 10, 它在二进制中是 1010, 所以其颠倒数是 0101, 就是 5. 但是在正常情况下, 5 是会写成 101 的, 所以 5 的颠倒数仍然是 5, 而不是 10. 但是, 我们又不能规定把 5 写成 0101, 因为这样一来 5 就不是回文数了, 而它应该是的.

这是不是意味着没有人会有兴趣去证明确有无穷多个素回文数了? 完全不是. 可以很容易地证明小于 n 的素回文数的个数在 $\sqrt{n}$ 附近, [与 n 比较, 这只占一个很小的部分. 在这样稀疏的集合里面去证明关于素数的结果, 是难得出了名的, 所以解决这样一个猜想将是一个突破. 然而 "回文数" 的定义实在太人为造作了, 所以无法在一个数学证明里详细地使用这个定义. 解决这个问题唯一现实的希望是去证明一个广泛得多的一般结果, 使这个问题成为其许多推论里的一个. 这样一个结果将是奇妙的, 无可否认是有趣的. 但是如果总在想着回文数, 是发现不了它的. 所以最好试一试去提出一个更加一般的问题, 或者去找一个更自然的这一类的问题. 后一方面的一个例子是: 有没有无穷多个素数可以写成 m^2+1 的形式? 这里 m 是一个正整数.

一个好问题的最重要的特性可能就在于它的一般性: 一个好问题的解答, 时常会超越这个问题而有许多分支. 对于这种使人愉悦的性质, 也许 "可一般化" 是一个更准确的字眼, 因为一个极好的问题可能看起来很特殊. 例如 "$\sqrt{2}$ 是一个无理数" 这个命题只是关于一个数的. 但是一旦您知道了怎样去证明它, 对于怎样证明 $\sqrt{3}$ 也是无理数就不会有困难了. 事实上, 这个证明可以推广到广泛得多的一类数

(见代数数[Ⅳ.1 §14]). 很常见的一种情况是：一个好问题, 在您开始去想以前, 看起来是没有什么意思的. 然后就会体会到, 问这样的问题是有道理的：它可能是一个更一般的问题的 "第一个困难的情况", 或者是一大堆问题的选择得很好的例子, 而在这些问题里都会遇上相同的困难.

有时, 一个问题就只是问一件事①, 但是一个想去问一件数学上的事情的人, 心里对于答案如何已经会有一个好主意了. 一个猜想就是作者坚信但又无法证明的数学命题. 和对于问题一样, 有些猜想好于其他的：我们在 §8.1 中已经看到, 一个最好的猜想对于数学研究的方向会有重大的影响.

① "问一件事", 原文是 "just a question". 本节中, 作者用了很大力气说明怎样看待数学中的问题：其作用如何, 如何区别问题的好与不太好, 总之是使读者不要以为问题就是 $1+1=?$ 或者更难得多, 只有难易之别. 这在数学圈子里面本是常谈, 对于本书预想的读者就不一定了. 所以, 作者常用 problem 一词, 而 question 则用得较少. 这也不能说是一个规矩, 而汉语翻译时又难以区别这两个词, 所以这里揣度了作者的意图, 用了 "问一件事" 的译法. 前面也有类似的情况. —— 中译本注

第II部分 现代数学的起源

II.1 从数到数系

Fernando Q. Gouvêa

自从人们会书写，就一直在记数字. 在每一个发展了一种记录信息方法的文明里，都可以找到一种记录数字的方法. 有些学者还认为，是先有了记录数字的方法.

有一点很清楚，数字首先是作为形容词出现的，用来确定某一种东西有几个或者有多少. 比方说，人们谈起例如有三个杏子比谈起数字 3 要早很多. 但是，一旦“三性”被摆到桌面上，使得这个形容词同样可以用来表示三条鱼、三匹马，一旦发展了一个书面记号“3”用于这三种情况，就有了 3 作为一个独立的实体出现的条件. 一旦如此，就是在做数学了.

每当引进一种新类型的数时，这个过程就会重复出现，首先是应用这个数，然后就用符号表示它，最后就把它自身接受下来作为类似实体的系统里的一员.

1. 古代数学里的数

我们所知道的最早的数学文献可以追溯到古代中东的埃及和美索不达米亚[①]文明. 在这两个文化里，都有一个专门从事书记工作的人的阶层. 书记员负责保存记录，这项工作时常要求他们会算术和解决简单的数学问题. 从这些文化里得到的数学文献绝大部分似乎是为了作青年书记员教学所用，其中许多都是以问题集形式出现的，而且附有答案和简单的解法. [美索不达米亚的这些文献是刻在一块泥板上的]，有一块泥板刻的是 25 个关于掘壕沟的题目，另一块上刻有 12 个需要用一次方程求解的题目，第三块刻的是关于正方形及其边的题目.

数字既是作为计数工具之用，也是作为量度工具之用，所以对于分数的需要必定很早就出现了. 把分数写下来是很复杂的事，而用它们来做计算更是困难的事情. 所以，“破裂的数”的问题，必定是第一个真正具有挑战性的数学问题. 人们是怎样

①美索不达米亚是 mesopotamia 的音译. 这个词是由两个希腊词构成的. 字首 meso- 意思是“之间”，字尾 -potamia 意思是“河流”. 所以这个名词的意译就是“两河流域”，两河就是底格里斯河与幼发拉底河，“两河流域”就是现在伊拉克及其附近的广阔地区. 古代先民在这里建立过许多王朝，巴比伦只是其中之一，也是最广为人知的一个. —— 中译本注

写分数的呢? 埃及人和美索不达米亚人提出了惊人不同的两种答案, 二者都与今天的写法颇为不同.

在埃及 (以及后来的希腊和地中海世界很大一部分), 基本的概念是 "n 分之一", 例如 "六的三分之一是二". 在这种语言下, 例如 7 除以 3 的思想就表述为: "七的三分之一是多少?" 答案则是 "二又三分之一", 还有一个附加的限制更是增加了复杂性, 在最终答案里, 同一类的 [用今天的语言来说就是同分母的] 分数只能用它的单数形式. 所以, 现在写成 "二个五分之一" 的数, 要写成 "三分之一和 [就是加] 十五分之一".

在美索不达米亚, 我们看到一个很不相同的思想, 它的出现可能是由于用它作不同类的单位的转换比较容易. 首先, 巴比伦人有一个办法来生成从 1 到 59 这些数目. 对于更大的数, 他们用一种进位制, 很像现在所用的进位制, 但是是以 60 为基础, 而不是以 10 为基础. 所以, 像 1,20 这样的写法, 就表示一个 60 和 20 个单位, 就是 $1 \times 60 + 20 = 80$. 同样的系统又推广到分数上面, 所以 "半个" 就要表示成 30 个 60 分之一. 用一个分点 ";" 来表示分数部分由此开始是很方便的, 虽然分点和逗号都只是现代的规定, 而在原来的文献里是没有的. 所以, 例如 1;24,36 就表示 $1 + \frac{24}{60} + \frac{36}{60^2}$, 也就是我们常写的 $\frac{141}{100}$, 即 1.41. 美索不达米亚的记数法称为六十进位制, 而与我们常用的所谓十进位制类似.

这两个系统都不足以处理复杂的数. 例如, 在美索不达米亚, 只用到**有限的**六十进位制式子, 所以书记员写不出 7 的倒数的准确的值, 因为 1/7 没有有限的六十进位制式子. 在实践上, 这就意味着用 7 去除就需要找到一个近似的答案. 另一方面, 埃及的 "几分之一" 系统则可以表示出任意正的有理数, 但是, 这样做就需要一串分母, 看起来十分复杂. [埃及的数学文献是记在一种所谓纸草书上的]; 有一本现存的纸草书包含了一些题目, 看来就是设计来求这种复杂的答案的. 有一个题目答案就是 "14, 4 分之一, 56 分之一, 97 分之一, 194 分之一, 388 分之一, 679 分之一, 776 分之一." [用现代的方法作加法, 就知道] 这个数如果用现代记号来表示, 就是分数 $14\frac{28}{97}$. 看来在数学发展的很早时期, 为计算而计算的快乐就已经相当根深蒂固了.

地中海文明在相当一段时期里, 把这两种系统都保存下来了. 绝大部分日常的数用 "几分之一" 系统来记. 另一方面, 天文学和航海需要更大的精确性, 所以在这些领域里采用了六十进位制, 其中包括时间和角度的量度. 现在把一小时分成六十分钟, 一分钟分为六十秒, 都可以经过希腊天文学家追溯到巴比伦的六十进位制分数. 将近四千年来, 我们至今还在受着巴比伦书记员的影响.

2. 长度并不是数

在古希腊时期和希腊化时期[①]的文明里, 数学变得更加复杂了. 当然, 希腊人因为第一个提出数学证明而闻名. 试图利用清晰的初始的假设和细心的命题, 以严格的演绎方法研究数学, 他们是第一个民族. 可能正是由此, 他们对于数及其与其他量的关系特别小心.

大约在公元前 4 世纪的相当一段时间, 希腊人得出了 "不可通约量" 这个重要发现. 就是说, 他们发现了把两个已给的量表示成为第三个量的 (整数) 倍, 并不一定能做到. 这并不仅是说, 长度和数在概念上是不相同的 (当然, 这一点也很重要), [更重要的是] 希腊人还对不能用数来表示长度给出了证明.

他们是这样来论证的. 如果两条线段的长度可以用数来表示的话, [因为当时人们对于数, 最多知道有分数], 则在最坏的情况下会用到一些分数. 然后, 改变长度的单位, 就可以断定, 这两个长度都相应于完整的数. 换句话说, 一定可以找到一个长度单位, 使得两条线段包含这个单位的个数都是完整的数. 这时就说, 这两条线段可以 "同时度量", 也就说, 它们是 "**可通约的**".

然而, 玄机在于希腊人还会**证明**两个数并不一定总是可通约的. 他们的标准的例子是关于正方形的边和对角线 [的情况, 这时就找不到共同的长度单位]. 我们并不确切知道希腊人当时是怎样发现它们是 "**不可通约的**", 但是很可能是这样思考的: 若从对角线减去边长 [即在长的线段中减去短的线段], 就会得到一个短于二者的线段 [即余量]; 如果对角线和边可以用同样的单位来度量, 它们的差当然也如此. 现在对上面得到的余量和正方形的边再重复上面的程序, 即从正方形的边减去第一次的余量 [(仍是从长的减去短的)] 多次, 例如减了两次, 直到第二次的余量又短于第一次的余量为止. 第二次的余量仍然可以用公共的单位来度量. [于是就看还有余量没有. 如果仍然有, 就再从第一次的余量减去这个新的第二次的余量多次, 直到新的余量又比第二次的余量短为止. 结果是: 或者减尽了, 再也没有余量, 或者减不尽, 就有了第三次的余量, 于是再从第二次的余量中多次减第三次的余量, 并如此以往]. 结果是: 这个过程永远不会终结; 相反, 它会产生出越来越小的余量线段. 最后, 余量会短于公共的单位. 但原来的推理说明了余量中包含的公共单位的段数仍然是完整的数, 而这是不可能的 (说到头, 任何完整的数都不会小于 1), 所以, 我们就能断定, 这个公共单位事实上不存在.

当然, 对角线也有长度. 今天我们会说: 若边长是一个单位, 则对角线长是 $\sqrt{2}$

---

①古希腊时期是指公元前 3—4 世纪以前的希腊时期. 人们认为这是希腊文化的黄金时代. 当时的希腊是城邦国家, 而苏格拉底、柏拉图、亚里士多德都是那个时期的思想家, 也就是希腊文化的代表人物. 欧几里得几何学就是这个时期数学的代表作. 希腊化时期以亚历山大大帝去世为起点到罗马人灭亡了希腊为止, 也就是围绕着亚历山大里亚城兴起的时代, 它是希腊文化的高峰, 但是又与古典的希腊文化有很大区别. 这以后罗马帝国灭了希腊, 人类历史又到了一个新时期. —— 中译本注

个单位, 这样, 上面的论证就说明 $\sqrt{2}$ 不是一个分数. 希腊人并不真的知道 $\sqrt{2}$ 在什么意义下也是一个数. 相反地, [希腊人认为] 它是一个长度, 或者更好是说, 它是对角线长度和边的长度之比. 把类似的论证用于其他的长度, 例如他们还知道面积为 1 的正方形的边长和面积为 10 的正方形的边长也是不可通约的.

于是, 结论就是: 长度并不是数, 相反, 长度是另一类 "大小", 即是另一类的 "量". 但是现在我们知道所谓 "量" 的种类是在扩散, 其中有数, 有长度, 有面积, 有角度, 有体积等等. 每一个都必须看成是不同类别的量, 而彼此不能比较.

这对于几何学就成了一个问题, 特别是在量度事物时成了问题. 希腊人解决这个问题, 很关键地依赖比的概念. 同一类的量有比, 而且还允许这个比等于两个另一类的量的比, 两个比要相等, 这要用到欧多克索斯 (Eudoxus) 的比例理论, 而这个理论是希腊几何学里最重要最深刻的思想之一. 所以, 例如希腊人不说有一个数叫做 π, 因为 π 对于他们并不是一个数, 他们的说法是: "一个圆 [的面积] 与立在它的半径上的正方形的面积之比, 等于这个圆的圆周与直径之比". 注意, 这两个比, 前一个是两个面积的比, 后一个是两个长度的比. [面积和长度则是不同类的量]. 在希腊数学中, 数 π 并没有特别的名字, 但是希腊人把它与数的比加以比较, 阿基米德[VI.3] 指出, 它略小于 22 对 7 之比, 略大于 223 与 71 之比.

这种做法在我们看来很笨拙, 但是希腊人用得很好. 此外, 能够把许许多多的量组织到不同的类别 (线段、角、曲面等等) 里去, 这样的想法在哲学上很令人满意: 同一类的量可以用比来互相关联起来, 各种各样的比又可以互相比较, 这些都是发生在我们意念中的事物. [这是一种 "理" 或者叫 "道"], 所以, 不论在希腊文中还是在拉丁文中, 比这个词和表示 "理由" 或 "解释" 的词是一样的(在希腊文中, 这个词是 logos, 在拉丁文中是 ratio). [无理数, 英语作 irrational, 其中的] "irrational" 一词 (希腊文作 alogos) 从一开始, 就既可以表示 "没有比", 也可以表示 "没有道理".

这种一丝不苟的理论系统不可避免地与实际量度例如长度、角度等日常需要脱节. 天文学家还是继续用他们的六十进位制近似, 画地图的人和其他科学家也还是我行我素. 当然也有 "漏网之鱼", 公元 1 世纪亚历山大里亚的海伦 (Heron of Alexandria) 就写过一本书, 读起来似乎是想把理论家的发现用于实际的量度. 例如, 推荐用 22/7 作为 π 的近似值应该归功于他 (很可能, 他之所以选用阿基米德的上界, 是因为它是一个比较简单的数). 然而, 在理论数学里, 数和其他种类的量的区别仍然很坚固.

古希腊时期以后, 我们可以看到, 在西方超过 1500 年的历史中, 有两个主要的主题: 第一, 希腊人把量分为不同的种类, 这种划分慢慢地被废除了; 第二, 为了做到这一点, 数的概念一再地被推广.

3. 十进位值

表示完整的数的系统最终要归功于印度次大陆的数学家. 公元 5 世纪前 (说不

定还要早很多), 印度人创造了九个符号来表示一到九这些数码, 还应用这些数码的位置来表示它们的真的值. 这样, 在个位上的 3 就表示三, 而在十位上的 3 则表示三十. 这当然也就是现在仍然在应用的; 虽然符号已经变了, 但是原理未变. 大约同时, 还发展了定位记号来表示空位, 这个记号最终就演化为零.

印度天文学广泛地应用正弦, 而正弦几乎从来不是完整的数. 为了表示它们, 使用了一种巴比伦式的六十进位系统, 即每一个六十进位的数码都用十进位系统来表示. 这样, "三十三和一象限" 就可以写成 33 15′ 就是 33 个单位加上 15"分"("分" 是六十进制的概念, 就是六十分之一).

十进位值的记数法很早就由印度传到伊斯兰世界. 在 9 世纪的巴格达新建立的哈里发[1], 有一个叫做阿尔 · 花拉子米[VI.5] 的人写了一本论印度式记数法的书, 就 "用了九个符号". 几个世纪以后, 阿尔 · 花拉子米 (Al-Khwārizmi) 的书被译成了拉丁文, [书名《印度计算术》(*Algoritmi de Numero Indorum*)]. 此书中世纪后期在欧洲如此流行, 以至于十进位制记数法时常就被叫做 "algorism", [其实就是 Algoritmi, 即阿尔 · 花拉子米. 算法一词也就是由此来的].

最值得我们注意的是, 在阿尔 · 花拉子米的书中, 零仍然处于特殊的地位. 它是一个定位记号, 而不是一个数. 但是, 一旦有了一个记号, 而且我们又用它来做算术, 定位记号和数的区别很快就消失了. 要做多位数的加法和乘法, 就需要知道怎样用零去加、去乘. 就这样 "无" 也就慢慢地变成了一个数.

4. 人们需要的是数

当希腊文化被其他影响代替时, 实用的传统就更加重要了. 这一点可以从阿尔 · 花拉子米的另一本著名的书 ("代数" 一词就是从这本书的书名得来的[2]) 看出来. 这本书实际上是许多不同类型的实用或半实用问题的概要. 阿尔 · 花拉子米在书中开宗明义地宣布, 我们不再是生活在希腊数学的世界里, "当我考虑人们在计算中需要的是什么时, 我发现人们需要的是数".

阿尔 · 花拉子米的书的第一部分是讨论二次方程, 以及处理二次方程所需的代数计算 (当然都是用文字来表述的, 什么符号也没有用). 他的方法实际上就是现在还在使用的二次方程公式, 当然其中就需要求平方根. 但是, 在每一个例子里, 需要求平方根的数都是完全平方数, 所以平方根很容易求 —— 阿尔 · 花拉子米得到的确实是一个数!

然而, 在这本书的其他地方, 就可以看到阿尔 · 花拉子米已经开始把无理的平方根看成类似于数的实体. 他教导读者怎样对含有平方根的符号进行操作, 而且给

---

①哈里发 (Caliphate) 一词是指伊斯兰的国王的职务或其领地. —— 中译本注

②这本书是用阿拉伯文写的. 原名 *HIsab al-jabr W'al-muqubalah*. *al-jabr*, 意为还原, 用现代语言来说, 就是 "移项". 后来此书译为拉丁文, 书名为 *Liber Algerae et Almucabala*. 现在统称为《代数学》. 代数, 英文是 algebra , 就是从阿拉伯文的 al-jabr 和拉丁文的 algerae 来的. —— 中译本注

出例如下面那样的例子：$(20-\sqrt{200})+(\sqrt{200}-10)=10$(当然都是用文字来进行). 在书的处理几何和量度的第二部分, 甚至可以看到对于平方根的近似："乘积为一千八百七十五; 取它的根, 这是一个面积; 它是四十三多一点."

中世纪的伊斯兰数学家不仅受到以阿尔 · 花拉子米为代表的实用的传统的影响, 也受到希腊传统的影响, 特别是欧几里得[VI.2] 的《几何原本》的影响. 在他们的著作里, 人们可以找到希腊的精确性和比较实用的量度方法的混合物. 例如在奥马尔 · 哈亚姆 (Omar Khayyam) 的《代数》一书里, 就既有希腊风格的定理, 又有求数值解的愿望. 在对三次方程的讨论中, 哈亚姆既努力用几何作图的方法来求解, 又哀叹自己不能找到数值.

然而, "数" 的领域已经在慢慢地扩大. 希腊人可能还是坚持 $\sqrt{10}$ 不是一个数, 而只是一条线段的名称, 即面积为 10 的正方形的一边, 或者是一个比. 在中世纪的数学家中, 不论是伊斯兰还是欧洲的数学家, $\sqrt{10}$ 的性态都越来越像一个数, 它进入了运算, 甚至出现在某些问题的解答里.

5. 对所有的数都给以同等地位

把十进制系统推广到分数, 这个思想是几位数学家互相独立地发现的, 其中最有影响的要推斯特凡(Simon Stevin, 1548—1620)[VI.10]. 他是弗兰德斯的数学家和工程师①. 他在 1585 年出版的一本名为 *De Thiende*(原书为弗莱芒语, 后来译为英语, 书名《十进算术》) 的小书中, 普及了这个推广了的十进制系统. 他把十进制推广到十分位、百分位等等, 就创立了现在仍在使用的十进制小数. 更重要的是, 他解释了这个系统如何用于简化涉及分数的计算, 给出了许多实际应用. 事实上, 书的封面上就宣布此书是为了 "占星学家、测绘人员和地毯的量度者之用".

斯特凡肯定知道他的举动所引起的某些问题. 例如他知道 1/3 的十进小数展开是无限的. 他的讨论只是说, 尽管完全的无限的展开是正确的, 但是在实际应用时加以截断不会造成多大的影响.

斯特凡也知道他的系统给出了一个方法, 对每一个长度都提供一个 "数"(指十进小数展开式), 他看不出 1.176 470 588 2 与 $\frac{20}{17}$(前者是后者的小数展开式的前一部分) 有什么区别, 也看不出 $\sqrt{2}$ 与 1.414 213 562 3(后者是前者的小数展开式的前一部分) 有什么区别. 在《算术》一书 (就是《十进算术》) 中, 他大胆地宣布, 所有的 (正) 数都是平方数、立方数、四次方幂的数等等, [所以都能开方, 而且开方以后] 所有的根也都是数. 他还说："没有什么荒唐的数、没有道理的数、不正规的数、无

①弗兰德斯 (Flanders) 就是荷兰和比利时北部交界处说弗莱芒语 (Flemish) 的地区, 所以文献中多说他是弗兰德斯数学家, 其实就是荷兰数学家. —— 中译本注

法研究的数, 或者无法听闻的数."[①] 这些称谓都是无理数的各种名称, 而无理数就是非分数的数.

于是, 斯特凡所提出的就是要把"量"或者"大小"的种种多样性都摆平, 汇合成一个包罗所有的以十进制展开式来定义的数的概念. 他知道, 这些数可以用一条直线上的长度来表示, 这就相当于现在相当清楚的称为正实数的概念.

斯特凡的建议由于对数的发明产生了大得多的影响. 对数和正弦、余弦一样, 是实际计算的工具. 为了应用这些工具, 就需要制表, 而表就需要用十进制小数来表示. 很快, 人人都使用起了十进制表示. 但是, 到晚得多的时候人们才了解, 这个举动是多么大的跃进. 正实数不仅是构成大一点的数系, 而且构成了大得不可比拟的数系, 它的内部的复杂性至今还没有被完全理解 (见集合理论[IV.22]).

6. 真的, 假的, 虚的

当斯特凡在写作时, 以后的步骤也在进行: 在方程式理论的压力下, 负数和复数都变得有用了. 斯特凡本人就已经意识到负数, 虽然很明显, 他并不喜欢负数. 例如他是这样来解释 -3 是方程 $x^2+x-6=0$ 的根的, 他说, 这就是指的 3 是相关的方程 $x^2-x-6=0$ 的根, 后一个方程是在前一个方程中用 $-x$ 代替 x 而得到的.

这自然是一个简单的逃遁之道, 但是三次方程式就产生了更困难的问题. 由于 16 世纪好几位意大利数学家的工作, 得出了一个求解三次方程式的方法. 关键的一步里包含了求一个平方根. 问题在于需要求其平方根的数, 有时是负数.

在那以前, 如果一个代数问题导致求某个负数的平方根, 则这个问题总是无解的. 但是方程式 $x^3=15x+4$ 确实是有解的 —— $x=4$ 就是一个解 —— 而在对它应用三次方程式的公式时, 就需要算出 $\sqrt{-121}$.

另一位意大利数学家和工程师庞贝里[VI.8] 决定来啃这块硬骨头, 看一看究竟发生了什么事. 在他的 1572 年出版的《代数学》一书里, 他硬着头皮往前闯, 计算了这个"新的根式", 而且发现这样就可以找到三次方程式的解. 这表明, 三次方程式的公式这时仍然能用, 更重要的是表明了这些奇怪的新数也可以是有用的.

要使人们对这些新的量感到舒服需要一段时间. 大约五十年后, 我们发现, Albert Girard (1595–1632, 生于法国死于荷兰的数学家) 和笛卡儿[VI.11] 都说, 方程式可以有三类根: 真的 (意为正根)、假的 (意为负根) 和虚的. 还不完全清楚, 他们所理解的虚根是否就是现在的复数根; 至少, 笛卡儿有时说, 一个 n 次方程式一定有 n 个根, 那些既不"真"又不"假"的根一定是虚根.

---

①这些称谓现在都已经很难听到了. 例如最后一个说法, 原书作 surd, 在老一点的代数书上还见得到, 即是"不尽根式". 此词出自前面说到过的阿尔 · 花拉子米的《代数》一书, 其中讲到无理数时说它们就是无法听闻的数. 后来译成拉丁文时, 就是 surdus(英文就是 inaudible, 无法听闻的意思), surd 就是由此而来的. 我们无法追究正文中那些说法的来历, 只好直译了. —— 中译本注

然而, 复数也慢慢地被人使用了, 它出现在方程式的理论中, 出现在关于负数的对数的辩论中, 而且与三角函数有关. 通过指数函数而与正弦和余弦函数的联系, 复数在 18 世纪成了欧拉[VI.19] 的有力工具. 到 18 世纪中叶, 人们都知道了, 每一个多项式都有一组完全的复数根. 这个结果以代数的基本定理[V.13] 知于世. 最后, 高斯[VI.26] 给出了大家满意的证明. 这样, 方程式的理论并不要求数的概念再有任何推广.

7. 数系, 老的和新的

因为复数与实数明显不同, 它们的出现就刺激人们开始把数分成不同的类别. 斯特凡的平等主义确实有影响, 但是不能消除完整的数要比十进制小数好, 分数要比无理数好这样的事实.

到了 19 世纪, 种种新思想要求对于数的分类作更仔细的考察. 在数论方面, 高斯和库默尔[VI.40] 开始考虑那些在某方面类似于整数的复数所成的集合, 例如所有形如 $a+b\sqrt{-1}$ 而 a 和 b 均为整数的复数的集合. 在方程式理论方面, 伽罗瓦[VI.41] 指出, 为了对方程式的可解性作细心的分析, 就必须对于哪些数可以算作是 "有理的" 取得共识. 这样, 例如他就指出, 在阿贝尔[VI.33] 关于五次方程式不可解的定理中, "有理" 就是指 "可以表示为多项式之商, 而且这些多项式是指以原方程系数为符号的多项式", 他还指出, 这些表达式的集合服从通常的算术的规则.

在 18 世纪, 兰伯特 (Johann Heinrich Lambert, 1728–1777, 瑞士数学家) 证明了 e 和 π 都是无理数, 他还猜测, 它们事实上是超越数, 就是说它们不会是任何 [整数系数] 多项式方程的根. 当时, 甚至超越数是否存在也属未知; 1844 年, 刘维尔[VI.39] 证明了这种超越数确实存在. 不过几十年间, e 和 π 都是超越数也得到了证明, 而在 19 世纪末, 康托[VI.54] 证明了事实上绝大多数实数都是超越数. 康托的发现第一次突出地强调了下面的事实: 由斯特凡所普及了的数的系统真是深不可测.

然而, 数的概念的最大的变化来自哈密顿[VI.37]1943 年发现一个全新的数系以后. 哈密顿注意到, 用复数 (而不是简单地用一对实数) 来将平面坐标化, 会大大地简化平面几何. 他就开始来找一个类似的途径来把三维空间坐标化. 这件事后来证明是不可能的, 但是把哈密顿引导到一个四维的系统, 他称之为四元数[III.76]. 这些四元数的性态很像是数, 但有一个关键性的区别: 乘法不是可交换的, 就是说, 若 q 和 q' 是两个四元数, 则 qq' 和 $q'q$ 一般是不相同的.

四元数是第一个 "超复数" 系, 而它的出现带来了许多新问题. 还有其他的这种数系吗? 什么才算是数系? 如果说某些 "数" 不能满足交换律, 那么能不能造出破坏其他规则的数来?

从长期来看, 这种智慧上的发酵引导数学家慢慢地放松了 "数" 或 "量" 这些模糊的概念, 而紧紧抓住代数结构这个比较形式的概念. 到头来, 每一个数系无非

就是一个可以在其上进行运算的实体的集合. 使我们感兴趣的是, 它们可以用来把我们关心的系统参数化, 或者说坐标化. 完整的数 (现在可以使用它的来自拉丁文的形式化的名字：整数) 可以用来把计数概念形式化, 而实数可用来把直线参数化, 从而成为几何学的基础.

到了 20 世纪初叶, 已经有许多著名的数系了. 整数傲居首位, 后面是逐步放大的层次：有理数 (即分数)、实数 (即斯特凡的十进制小数, 但是已经仔细地形式化了) 以及复数. 比复数更一般的还有四元数. 但是绝不是仅有这些数系. 数论学家搞出了几个不同的代数数域, 它们是复数的子集合, 但是又可以看作自治的系统. 伽罗瓦引进了一些有限的系统, 它们服从算术的通常的规则, 而现在就称之为有限域. 函数论专家要和几个函数域打交道, 他们肯定不认为这些是数, 但是它们和数的类同已经被人们看到了并研究过.

20 世纪初, 亨泽尔 (Kurt Hensel) 引进了*p 进数*[III.51], 它是从有理数中赋予素数 p 以特殊的作用而得出的 (因为 p 可以随意取, 所以事实上亨泽尔创造了无穷多个新数系). 它们也 "服从算术的通常的规则", 这句话是指加法和乘法的行事正如我们的预期. 用现代语言来说, 它们都是域. p 进数是事物的第一个这样的系统, 它们被承认为数, 但是又与实数和复数没有看得见的关系 —— 只有一点除外, 即它们都包含有理数. 结果是它们引导斯坦尼兹 (Ernst Steinitz, 1871–1928, 德国数学家) 创造了域的一般理论.

出现在斯坦尼兹的工作里的向着抽象化的运动在数学的其他部分也发生了, 值得注意的是群及其表示的理论以及代数数理论. 所有这些理论被*艾米 · 诺特*[VI.76] 汇集成一个概念的整体, 艾米 · 诺特的计划后来就称为 "抽象代数". 这门学科把数完全抛到后面, 而集中注意带有运算的集合的抽象结构.

今天, 要决定什么样才算是一个 "数" 已经不太容易了. 原来的序列 "整数、分数、实数和复数" 中的对象肯定要算是数, p 进数也算是数. 但是, 另一方面, 四元数极少有人把它们算是 "数", 虽然它们也被用来把某些数学概念坐标化. 事实上, 还有更奇怪的系统, 如凯莱的*八元数*[III.76] 也作为坐标而出现. 说到底, 什么可以用于把手头的问题坐标化, 我们就把什么 [作为数]. 如果这样的数系还不存在, 人们就会去发明它.

进一步阅读的文献

Berlinghoff W P, and Gouvêa. 2004. *Math through the Ages: A Gentle History for Teachers and Others.* expanded edn. Farmington, ME/Washington, D C:Oxton House/The Mathematical Association of America.

Ebbinghaus H -D, et al. 1991. *Numbers.* New York: Springer.

Fauvel J, and Gray J J, eds. 1987. *The History of Mathematics. A Reader.* Bas-

ingstoke: MacMillan.

Fowler D. 1985. 400 years of decimal fractions. *Mathematics Teaching*, 110:20-21.

— 1999. *The Mathematics of Plato's Academy*, 2nd edn. Oxford, Oxford University Press.

Gouvêa F Q. 2003. *p-adic Numbers: An Introduction*, 2nd edn. New York: Springer.

Katz V J. *A History of Mathemtics*, 2nd edn. Reading. MA: Addison-Wesley.

—, ed. 2007. *The Mathematics of Egypt, Mesopotamia, China, India and Islam: A Sourcebook.* Princeton, NJ: Princeton University Press.

Mazur B. 2002. *Imagining Numbers (Particularly the Square Root of Minus Fifteen).* New York: Farar, Straus, and Giroux.

Menninger K. 1992. *Number Words and Number Symbols: A Cultural History of Numbers.* New York: Dover(Translated by P. Broneer from the revised German edition of 1957/58: *Zahlwort und Ziffer. Eine Kulturgeschichte der Zahl.* Göttingen: Vandenhoeck und Rubrecht.)

Reid C. 2006. *From Zero to Infinity: What makes Numbers Interesting.* Natick, MA: A. K. Peters.

II.2 几 何 学

Jeremy Gray

1. 引言

关于几何学的现代观点是受到了希尔伯特[VI.63] 和爱因斯坦在 20 世纪初的新颖的几何学理论的启示, 而他们的理论又是来自几何学在 19 世纪根本性的重新陈述. 几千年来希腊人的几何学最突出地表现在欧几里得[VI.2] 的《几何原本》里, 成为完全的严格性的范式, 实际上是人类知识的范式. 新的理论完全颠覆了整个一种思维方式. 本文将要追随几何学的发展历史, 从欧几里得时代开始, 继之以非欧几何学的发明, 而终于黎曼[VI.49]、克莱因[VI.57] 和庞加莱[VI.61] 的理论. 沿着这个过程, 我们要考察几何学的概念是怎样和为何有如此引人注目的变化. 至于现代几何学本身, 本书以后各个部分会去讨论.

2. 朴素的几何学

一般说来, 几何学特别是欧几里得几何学, 总是被非正式然而正当地看成是对于我们周围的一切的数学描述: 这是一个 3 维空间 (左右、上下、前后) 似乎伸向无穷远处, 其中的对象各有位置, 而有时又会移动到别的位置, 所有这些位置都可以用沿着一些直线进行量度来确定: 这个对象离那一个 20 米远, 它有 2 米高, 如此等等. 我们也可以测量角度, 在距离与角度之间, 有一个微妙的关系, 这个关系我们看不见, 但是可以从推理得到. 几何学是一门数学学科, 里面充满定理 —— 等腰

三角形定理、毕达哥拉斯定理等等 —— 综合概括了关于长度、角度、形状和位置所能够说明的一切. 几何学的这一个侧面与绝大多数其他科学的区别在于它的高度演绎的本性. 确实好像是只需拿起最简单的概念, 对它们苦苦思索, 对于空间就能建立起一个给人深刻印象的演绎的知识体系, 而不必去收集经验证据.

但是这能行吗? 事情真是这么简单吗? 我们能不能不离开椅子一步就得到关于空间的真知? 结果是不行, 还有其他的也是以长度和角度为基础的几何学, 它有一切权利声称自己是有用, 但是与欧几里得几何学又不相同. 这是 19 世纪早期的一项惊人的发现, 但是想要有这样的发现, 对于一些基本的概念必须要给予精确的定义, 这些概念例如有直线的 "直"、长度、角度等等, 而这个过程花了好几百年. 一旦完成了这件事, 第一个新几何学就被发现了, 以后接着就有无穷多种新几何学.

3. 希腊几何学的形成

几何学可以看成对于世界的有用事实的汇集, 也可以看成是一个有组织的知识总体. 不论是哪种看法, 对于这门学科的来源都有很多争论. 很清楚, 埃及和巴比伦的文明至少都有一点几何学知识 —— 否则就不可能建起那些大城市、那些精心建造的庙宇和金字塔. 但是不仅是对于希腊人以前人们知道些什么很难得到丰富详尽的资料, 甚至对于柏拉图和亚里士多德时代以前仅知的零散资料也很难看懂. 原因之一是后来的希腊作者们所取得的伟大成就, 还有成为确定的几何教材的作者、亚历山大里亚的欧几里得 (约公元前 300 年) 取得的伟大成就, 这些成就太伟大太蔚为壮观了. 只要稍微翻阅一下他的《几何原本》就会知道, 对几何学历史的恰当的陈述必须远远超出仅仅知道如何获取几何事实.《几何原本》是一部组织严密的演绎的知识体系, 它分成若干不同的主题, 但每一个主题都有复杂的理论结构. 这样, 不论几何学的来源如何, 到了欧几里得的时代, 它已经变成了合乎逻辑的学科的范式, 提供的是这样一种知识: 与从日常经验中直接收集来的知识相比较, 不仅颇为不同, 而且要更高.

因此, 本文不打算详细讨论几何学的早期历史, 而是循着最直截了当的途径直击几何学最引人注意之处: 数学知识表观上的确定性. 正是由于这一点, 几何学有权声称自己是高一级的知识, 从而导致了后来非欧几何这个了不起的发现, 除了欧几里得几何学以外, 还有其他的几何学, 每一点上都是同样严格地符合逻辑. 更值得注意的是, 其中有一些已被证明提供了比欧几里得几何学更好的关于物理世界的模型.

《几何原本》从前四卷研究平面图形开始: 三角形、四边形和圆. 著名的毕达哥拉斯定理就是第一卷的第四十七个命题. 接着的两卷讲比和比例的理论以及相似形 (即图形的经过缩放的复本) 的理论, 对它们的处理是高度精巧的. 下面的三卷是关于完整的数, 似乎是对现在看成初等数论的更早期材料的重新处理. 例如在这

里就有素数的个数为无限这一著名结果. 第十卷是最长的一卷, 讨论一个看来很特殊的长度为形如 $\sqrt{a \pm \sqrt{b}}$(这是现代的写法) 的线段. 最后三卷是关于 3 维空间的几何学, 第十卷写得那么长, 就在这里起了作用. 全书以五个正多面体的作图以及再没有其他正多面体存在结束. 第五个也就是最后一个正多面体的发现是使得柏拉图大为激动的主题. 说真的, 五个正多面体对于柏拉图的宇宙论是很关键的, 可见柏拉图晚年的著作《蒂迈欧篇》.

《几何原本》的多数卷都是以各个定义开始的, 而每一卷都有很精巧的演绎结构. 例如, 要理解毕达哥拉斯定理, 就要倒推到前面的结果, 然后又推到更早的结果, 直到最后停留在基本的定义上. 整个结构迫使人不得不接受, 英国哲学家霍布斯 (Thomas Hobbes, 1586–1679) 在已经是成年的时候读了它, 一下子就从不信转变为终生的信仰. 《几何原本》如此服人之处, 就在于它所使用的论证的本性. 除了少数例外 (大多是在关于数论的几卷里), 这些论证都是用的公理方法. 这就是说, 这些论证从一些非常简单的公理开始, 公理是假设自明地为真的, 然后用纯粹的逻辑手段由这些公理导出定理.

为了使这种途径能起作用, 必须要具有三个特性. 第一个是要避免循环论证. 就是说, 如果想要证明一个命题 P, 就得从一个早前的命题来推导它, 而这个早前的命题又要从一个更早的命题导出, 如此等等, 但是, 在任何时刻都不能再回到命题 P. 如果是那样的话, 就没有从公理导出 P, 而仅仅是证明了推理链条上的各个命题都等价. 在这方面, 欧几里得做了非常出色的工作.

第二个特性是推理的规则必须清晰而且可接受. 有些几何命题看来如此明显, 使得人们没有注意到, 它们还需要证明, 在理想情况下, 人们不应该使用图形的没有在定义里清楚表明的性质, 但是要符合这个要求是很困难的事. 欧几里得在这方面的成功就不那么给人以深刻印象, 而是瑕瑜互见. 从一方面看,《几何原本》是一部了不起的著作, 在它所覆盖的所有主题上, 都远远超过同时代的讲法, 而能够垂之千年. 另一方面, 它又有小的瑕疵, 让后来的评论者不时加以补正. 例如, 对于两个圆, 当一个圆的圆心位于另一圆外, 而且半径之和又大于两圆心的距离时, 两圆必定相交, 对此《几何原本》既没有明确的假设, 也没有证明. 然而, 欧几里得惊人地清楚, 有一些推理法则具有广泛的甚至是普适的可应用性, 另一些规则则适用于数学, 因为它们依赖于其中涉及的名词的意义.

第三个特性与第二个不能完全分离, 就是它包含了充分多的定义. 欧几里得提出了两种或者三种定义. 卷 I 一开始就是关于其对象的七个定义, 例如 “点” “直线”, 它们被认为是原始的, 因此不需定义, 而近年来的研究说明, 这些定义可能是后人加上去的. 然后, 就给出一些熟悉的图形的定义, 它们在卷 I 中就已经给出了, 而在以后各卷中又一再出现, 如 “三角形” “四边形” “圆” 等等, 以便对它们可作数学的处理. 卷 I 中的 “公设” 构成第三类定义, 这里面就有问题了.

卷 I 提出了五个 "共同概念", 它们是一种具有非常一般性质的推理规则. 例如, 其中有 "如果等量被加到等量上, 则所得的总量仍相等". 此卷里又提出了五个 "公设", 它们具有比较狭窄的数学性质. 例如第一个公设: 从任意一点到任意另一点可以连一直线. 这些公设中有一个, 即第五公设后来就恶名昭著了, 这就是所谓的平行线公设: "若一直线与另两直线相交, 而使同一侧的两个内角 [之和] 小于两直角, 这两条直线若无限制地延长, 必相交于内角 [和] 小于两直角的一侧".

所以, 平行线就是不相交的直线. 苏格兰的编者 Robert Simson①引进了平行线公设的一个有帮助的重新陈述, 发表在他于 1806 年所编辑的《几何原本》里, 他指出, 如果假设《几何原本》中不依赖于平行线公设的那一部分仍然成立, 则平行线公设等价于以下的命题: "给出平面上任意直线 m, 以及此平面上任意的不在 m 上的点 P, 则平面上经过 P 必有恰好一条直线 n 不与 m 相交". 从这个陈述可以清楚地看到, 平行线公设作了两个论断: 给定直线和点如上所述, 则必有一条平行线存在, 而且此平行线是唯一的.

值得注意的是, 欧几里得本人大概也感到平行线公设笨拙难用. 它的断言是希腊数学家和哲学家都不喜欢的性质, 也许这可以解释何以平行线公设在卷 I 中出现那么晚, 一直拖到卷 I 的命题 29. [《几何原本》的著名] 评论家普罗克鲁斯 (Proclus, 约公元 5 世纪的数学家) 在他关于《几何原本》卷 I 的广泛的评论里就观察到: 当一条双曲线和它的渐近线向外运动时, 就相距越来越近, 但是永不相遇. 如果一条曲线和一条直线可以如此, 为什么两条直线就不可以在向外运动时, 越来越近但永不相遇呢? 这件事需要进一步的分析. 不幸的是, 如果数学家抛弃了平行线公设, 而退却到其余定义的推论中去, 《几何原本》也就所余无几了, 因为有很大一部分知识依赖于它. 最值得注意的是, 要证明三角形内角和为二直角, 就需要平行线公设 —— 在证明许多有关图形中的角的定理包括毕达哥拉斯定理时, 都要用到关于三角形内角和的这个关键结果.

不论多少代的教育家对于欧几里得的《几何原本》作何评论, 很多专家都知道它是一个并不令人满意的妥协的产物: 可以得到一个有用而且非常严格的理论, 但是代价是需要接受平行线公设. 而平行线公设又是很难在信仰基础上接受的, 它既不像其他公理那样给人以直观上就显然成立的感觉, 又没有明显的方法来检验它. 一个人的标准越高, 这个妥协就越令他痛苦. 专家们就问了: 怎么办呢?

这里只需举出希腊人普罗克鲁斯的评论就够了. 在他看来, 如果说平行线公设并不显然, 而没有它几何学又太贫瘠, 那么唯一的可能性就是: 它之所以仍然是真

①在 18 世纪有很多人编辑《几何原本》以作教本之用, R. Simson 是其中之一, 他当时是格拉斯哥大学教授. 平行线公设的这种陈述究竟归属于谁, 似乎也有争论. 同为这个陈述, 多数文献上又说是 John Playfair 于 1795 年给出的, 而且争论双方似乎都能引经据典. 看来这种争论没有实质的意义, 列举于上, 仅供读者参考. —— 中译本注

的, 就是因为它是一个定理, [是可以证明的], 于是他就给出了一个证明. 他的论据如下：令两条直线 m 和 n 与第三条直线 k 分别交于 P,Q 两点, 而且内角之和为两个直角. 现在通过 P 点作直线 l, 指向 m 和 n 之间的空间. 当离开 P 点向远处运动时, l 和 m 的距离一定会增加, 所以直线 l 一定会与 n 相交.

普罗克鲁斯的论证是有毛病的, 这个毛病很微妙, 而且今后的 "证明" 所发生的毛病也大多由此开端. 他说 l 与 m 的距离会无限增长这一点是对的, 但是他的论证假设了直线 m 和 n 的距离不会也无限增长, 而相反会保持有界. 普罗克鲁斯知道得很清楚, 如果承认平行线公设, 则可以证明：如果直线 m 和 n 互相平行, 则它们之间的距离为常数. 但是在平行线公设得到证明以前, 没有什么能妨碍我们宣布直线 m 和 n 也会发散. 所以除非能够证明这两条直线既不相交也不会发散, 普罗克鲁斯的证明就起不了作用.

普罗克鲁斯并非具有这个企图的第一人, 但是他的论证是这类论证的典型. 这些证明都是把平行线公设从欧几里得的《几何原本》中除去, 同时也除去了所有依赖于他的论证和定理, 余下的部分称为《几何原本》的 "核心", 人们就是企图利用这个核心来把平行线公设作为一个定理来证明. 所以, 从普罗克鲁斯的企图能够导出的正确结论, 并非平行线公设作为一个定理而成立, 而只是假设知道了《几何原本》的核心, 平行线公设与以下命题是等价的, 即两条不相交的直线也不会发散. 一位 6 世纪的作者 Aganis(我们对他的生平几乎一无所知) 在后来的证明平行线公设的企图中, 假设了两条平行线互相处处等距, 所以他的论证只是证明了假设了《几何原本》的核心以后, 欧几里得关于平行线的定义等价于定义平行线即为互相等距的直线.

还要注意, 如果没有搞清楚直线的哪些性质来自它的定义, 而哪些性质则应作为定理来导出, 那就连辩论也无法进行了. 如果我们愿意一路走, 一路把关于几何学的种种假设都加到 "常识" 的存储中去, 那么《几何原本》的细心的演绎结构就会崩塌成为一大堆事实的累积.

欧几里得很清楚是把《几何原本》的演绎特性作为重要的东西来对待的, 但是, 我们还可以问, 他对几何学是干什么的又有何想法呢？例如, 几何学是否意味着对于空间作数学描绘呢？现存的文本都没有说到欧几里得是怎么想这个问题的, 但是有一点值得注意, 最著名的希腊宇宙理论, 由亚里士多德所创立, 后人又多有评论, 都假设空间是有限的, 而以恒星所在的球面为边界[①]. 《几何原本》的数学空间则是无限的, 所以至少可以考虑这样的可能性, 所有这些作者都没有打算以数学空间作为物理世界的简单理想化.

①亚里士多德的天体学说认为天有九层, 是九个水晶球面, 恒星在最外层, 称为 "永动天", 在那以外则是神的世界了, 所以本书正文说亚里士多德假设空间是有限的. —— 中译本注

4. 阿拉伯世界和伊斯兰世界的评论者

今天所说的希腊几何学实际上只是不多几个数学家在不到两个世纪的时期之内的工作. 它们后来被数量大得多, 而且分布在更广袤的区域、在更长时期的阿拉伯和伊斯兰世界的作者们所继承. 人们记得这些作者, 是作为希腊数学和科学的评论者, 并把这些传递给后来的西方作者, 但是也应该把他们也看作独立的创造的革新的数学家和科学家. 他们中有些人也拿起了欧几里得《几何原本》来研究, 其中也就包含了平行线公设问题的研究. 他们也认为这不是一个适当的公设, 而是可以只用核心即能证明的定理.

第一批有此企图者中有一个叫 Thābit ibn Qurra 的人, 他是一个来自阿勒颇[①]的异教徒, 后来在巴格达居住和工作, 公元 901 年死于巴格达. 本书篇幅只许可我们描述一下他的第一个途径. 他论证说, 如果有两条直线 m 和 n, 同与第三条直线 k 相交, 如果它们在 k 的某一侧互相靠近, 则在其另一侧必无限地发散开去, 他由此导出, 如果两条直线与斜截的直线所成的内错角 (即图 1 上标为 a, b 的两个角) 相等, 则它们不可能在截线的一侧互相靠拢, [因为如果能靠拢了], 则情况的对称性将使得它们在另一侧也靠拢, 但是他证明了它们在另一侧必定发散开去, 他由此导出了欧几里得的平行线理论. 但是他的论证仍是有毛病的, 因为他没有考虑到还有两条直线在两侧都发散开去的可能性.

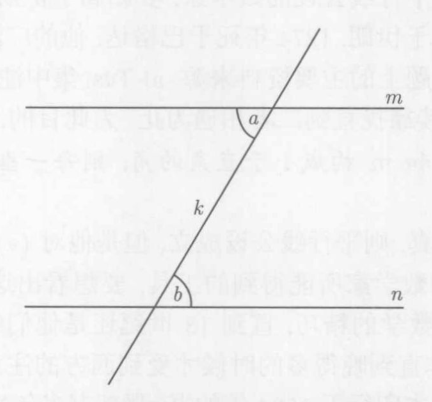


图 1 直线 m 和 n 与截线 k 构成相等的内错角 a 和 b

著名的伊斯兰数学家和科学家 Ibn al-Haytham 于 965 年生于巴士拉[②], 1041 年死于埃及, [也企图证明平行线公设]. 他取一个四边形, 使其有两个相等的侧边 AB 和 CD 均垂直于底边 BC(见图 2). 再从 A 点向对边作一垂线. 他企图证明这条垂

①阿勒颇 (Aleppo), 叙利亚北部的一个大城市, 有很古老的历史. —— 中译本注
②巴士拉 (Basra), 伊拉克最大的海港. —— 中译本注

线之长与底边 BC 相等, 由此就可以证明, 如果原来的两个垂直边之一, 例如 AB 向另一个 CD 移动, 它的顶就会扫出一条直线, 而与我们刚才作的垂线 AD 重合 (见图 2). 这就相当于说, 与一条直线处处等距的直线本身也是直线, 由此可以得到平行线公设. [这也就说明他的企图也失败了, 因为他也只能证明平行线公设与等距离直线的结果是等价的]. 他的证明后来被奥马尔 · 哈亚姆严厉批评, 因为他应用了运动的概念, 奥马尔 · 哈亚姆认为这个概念对于欧几里得《几何原本》实属异类. 它确实和欧几里得在几何学中对于运动概念的任意的应用很不相同, 因为在这时所得到的曲线 $AA'D$ 的性质并不清楚, 而这正是需要加以分析的.

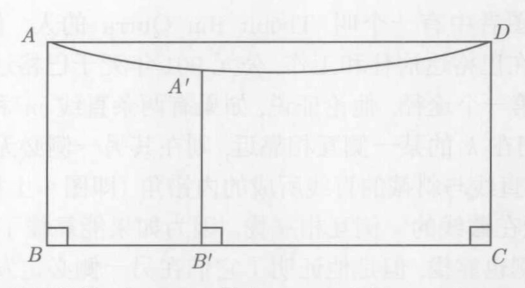


图 2　AB 和 CD 是相等的, 角 ADC 是直角, $A'B'$ 是 AB 向 CD 移动时中间的位置

最后一个企图证明平行线公设的数学家, 要归属于伊斯兰数学家 Nasir al-Dīn al-Tūsī. 他于 1201 年生于伊朗, 1274 年死于巴格达. 他的广泛的评论是我们对于早期伊斯兰数学在这个主题上的主要资料来源. al-Tūsī 集中注意于证明: 若两条直线开始靠拢, 则它们将继续靠拢直到二者相遇为止. 为此目的, 他开始来证明:

(*) *若两条直线 l 和 m 构成小于直角的角, 则每一垂直 l 的直线一定与 m 相交.*

他证明了若 (*) 为真, 则平行线公设成立, 但是他对 (*) 的证明是有毛病的.

如果只应用当时的数学家所能得到的工具, 要想看出这些论证究竟错在哪里, 真是一件难事. 伊斯兰数学的精巧, 直到 18 世纪还是他们的西方继承者未能超越的. 不幸的是, 这些著作直到晚得多的时候才受到西方的注意, 但有一个例外, 即在梵蒂冈的图书馆里的一本印行于 1594 年的书, 那部书多年来都被误认为是 al-Tūsī 的著作 (但可能是他的儿子的著作).

5. 对于《几何原本》的兴趣在西方的重新兴起

在西方, 对于平行线公设的兴趣重新兴起, 是随着 Commandino 和 Maurolico 所领导的翻译希腊文献的第二个高潮到来的, 这些文献由于印刷术的发明而广为传播. 在一些老的图书馆里发现了重要的文献文本, 这样就最终引导到《几何原本》的许多新版本出现, 其中有许多都谈到一点关于平行线的问题, 但是, [《圣经》的翻译

者]Henry Savile 一语中的, 他称之为 “对欧几里得的玷污”. 例如权力很大的耶稣会教士克拉维乌斯在 1574 年就重编了《几何原本》, 并在其中试图论证平行线可以定义为等距的直线①.

把物理空间很快地就确认为欧几里得几何学的空间, 是随着哥白尼天文学在 16 至 17 世纪逐渐被接受, 而所谓的恒星的天球, 即永动天被废除以后而来的. 牛顿[VI.14] 的《自然哲学的数学原理》一书已经成了这个空间学说的经典了, 在这部书里引力理论是坚定地站立在欧几里得空间里. 虽然牛顿的物理学要想得到接受还得经过战斗, 牛顿的宇宙论的道路却顺利得多, 成了 18 世纪谁也无法挑战的正统. 但是, 也可以论证说, 把物理空间确认为欧几里得几何的空间, 提高了赌注, 因为只要简单地从《几何原本》的核心得到的反直观的结论, 现在就可能成了物理空间的反直观的事实.

1663 年, 英国数学家沃利斯 (John Wallis, 1616–1703) 对于平行线公设采取了一种比他的先行者更加微妙的观点. 他曾就梵蒂冈图书馆里收藏的伪造的 al-Tūsī 的著作受教于哈雷, 因为哈雷是懂得阿拉伯文的. 沃利斯也企图给一个证明. 但是, 不寻常的是, 沃利斯也具有这样的洞察力, 能够看出自己的论证有毛病, 并且对此评论说, 他实际上证明的只是在有了核心以后, 平行线公设只是等价于断言有非全等的相似形存在. [而下面介绍的波尔约和罗巴切夫斯基的几何学, 就在否定平行线公设的条件下, 证明了所有的相似三角形都是全等的].

半个世纪以后, 继沃利斯而起的有平行线公设的最持久最彻底的保卫者萨凯里 (Gerolamo Saccheri, 1667–1733), 一个意大利耶稣会士, 他在自己去世的 1733 年出版了一本小书:《没有任何瑕疵的欧几里得》. 这本经典推理的小小杰作开启了一个三分法. 除非平行线公设已得到证明, 三角形的内角和既可以小于也可以等于或大于二直角. 萨凯里证明了 [在这三种可能性中], 如果某一种出现于一个三角形上, 则同一可能性必出现于所有三角形上. 第一种情况 (以下称为场合 L) 下, 每一个三角形的内角和都小于二直角. 第二种情况 (场合 E) 下, 每一个三角形的内角和都等于二直角. 第三种情况 (场合 G) 下, 每一个三角形的内角和都大于二直角. 场合 E 当然就是欧几里得几何, 萨凯里希望证明这是唯一可能的场合. 于是他就着手来证明: 另外两种场合都会独立地引起自相矛盾. 对于场合 G, 萨凯里成功地证明了确会引起矛盾, 然后他转向场合 L. 他说: “就只有它在阻碍 [平行线] 公理的真理

①克拉维乌斯 (Christopher Clavius), 是生于德国的耶稣会数学家. 他的功绩主要是领导了新历法 (格利高里历) 的制定, 他也主持重新编辑《几何原本》. 这个版本把《几何原本》分成 15 卷. 他是利玛窦的老师. 后来利玛窦和徐光启翻译《几何原本》为中文时, 就是用的这个版本. 所以在译本序言中说《几何原本》共分 15 卷, 而不是如我们知道的 13 卷. 这个序言中讲到利玛窦曾经受业于 “丁先生”, 其实就是克拉维乌斯. 这是因为克拉维乌斯是拉丁名字, 而他的德文名字至今不详. 有说是 Clau 或 Klau 或 Schlüssel. Schlüssel 意思是钉子或钥匙, 而 Clauvius 在拉丁文中的意思也就是钉子或钥匙, 利玛窦和徐光启就把他的名字译为丁先生. —— 中译本注

性了”.

场合 L 证明是很困难的, 萨凯里在研究过程中确立了许多有趣的命题. 举例来说, 如果场合 L 为真, 则两条不相交的直线有一条公共垂线, 而这两条直线在公垂线两侧都互相发散开去. 到最后, 萨凯里想依靠直线在无穷远处的动态的愚蠢的命题来克服这些困难; 正是在这里, 他的证明的企图失败了.

萨凯里的工作慢慢地但又没有完全地淡出人们的视野, 他引起了瑞士数学家兰伯特 (Johann Heinrich Lambert) 的注意, 兰伯特仍然追随着这个三分法, 但和萨凯里不同, 他没有停步于宣布自己证明了平行线公设. 相反, 他放弃了这一项尝试, 他的结果直到他去世以后, 在 1786 年才发表. 兰伯特仔细地区分哪些是难以理解的怪异的事情, 哪些是不可能的事情. 他有一个概要来证明在场合 L 下, 三角形的面积正比于两直角与内角和之差. 他知道, 在场合 L 下, 相似三角形必为全等三角形, 这就意味着天文学里用的三角函数表事实上并不成立, 对于大小不同的三角形, 需要有不同的表. 特别是对于每一个小于 60° 的角, 都恰好有一个等边三角形以它为顶角, 这就会引导到哲学家所谓的长度的 “绝对” 单位 (例如取顶角为 30° 的等边三角形的边长为这个绝对单位), 而莱布尼兹[VI.15] 的追随者沃尔夫 (Chritian Wolff, 1679–1754, 德国哲学家) 认为这种绝对单位是不可能存在的. 这确实是反直观的, 因为我们在谈到长度时, 总是把它定义为一个相对的量, 例如是巴黎的米尺的一定的比, 或是地球周长的一定的比, 或者其他类似的东西. 但是对于这些论据, 如兰伯特所说: “无论是出于爱或者恨, 数学家都毫无办法”.

6. 1800 年左右焦点的转移

西方对于平行线公设的兴趣潮起潮落, 高潮本来始于欧几里得《几何原本》的现代版本的出版, 现在又衰落了, 同时带来这项事业的新转机. 在法国大革命以后, 勒让德[VI.24] 着手来写一本教材为准备进入巴黎高工的学生之用, 这本教材打算把初等几何的教学恢复到某种类似于《几何原本》那样的严格的形式. 但是打算取代一部严重地依赖于直觉的书是一回事, 把它写成具有所需要的严格性的书却是另一回事. 后来勒让德认识到这一点, 而他的企图最终却失败了. 特别是他也和他的前人一样, 没有做到给平行线公设以足够的辩护. 勒让德的《几何学原理》(*Éléments de Géométrie*) 发行了多版, 每一版都对平行线公设有不同的讲法. 对于有一些讲法, 很难说好话, 但其中最好的确有极大的说服力.

勒让德的著作在精神上是古典的, 因为它仍然认为平行线公设必定为真是自然的事情. 但是到了 1800 年左右, 采取这种态度不再是普遍的了. 不是每个人都认为必须怎么样为此公设辩护, 有些人则心情镇定地对待另外一种想法: 平行线公设可能是不对的. 没有什么能比马堡大学的法学教授 F. K. Schweikart 在 1818 年给高斯[VI.26] 的短信更清楚地表明这种态度的了. 他在一页纸内讲了把他引导到所

谓 "星空几何学" 的主要结果, 在这种几何学中, 三角形的内角和小于两直角; 正方形必有特殊形状; 直角等腰三角形的高必有一定界限, Schweikart 把这个界限称为 "这个常数". Schweikart 走得这么远, 甚至宣布新几何学可能才是空间的真正的几何学. 高斯对此作了肯定的回应. 他接受了这些结果, 而且宣布, 只要把 "这个常数" 给出来, 他就能给出全部初等几何学. 有些人当然也不那么大度, 他们说 Schweikart 只不过是读过了兰伯特的遗著而已, 虽然他关于等腰三角形的定理是新的. 值得注意的在于心态: 这种新的几何学可以是真的, 而不只是一种数学奇谈. 欧几里得的《几何原本》再也不是一种桎梏了.

不幸的是, 高斯本人怎么想就远不是这么清楚了. 有些历史学家, 总记住了高斯突出的数学独创性, 倾向于这样来解释这项证据, 说高斯是发现非欧几何的第一人. 然而这点证据是微薄的, 很难由它得出可靠的结论. 有一些高斯在早年研究过欧几里得几何学的迹象, 包括对于平行线的新定义的研究; 高斯在晚年也曾经宣布过, 他多少年前就已经知道这个或那个结果, 还留下了他写给一些朋友的信. 但是在他留下的文稿里, 没有任何资料使我们能够重新描绘出高斯究竟知道什么, 或者可以支持宣布高斯发现了非欧几何.

情况大概是高斯在 1810 年代就认识到, 所有此前从欧几里得几何学的核心导出平行线公设的努力都已经失败, 而在将来, 所有这种努力也会失败. 他越来越坚信, 空间会有另一种可能的几何学. 在他的心目中, 几何学已经不再有算术那样的地位, 因为算术只是逻辑的问题, 而几何学和力学一样, 是一门经验科学. 在整个 19 世纪 20 年代, 高斯的立场最简单的准确表述就是他不再怀疑空间可以用一种非欧几何来描述, 而非欧几何只有一种, 就是上面说过的场合 L. 这是一个经验的问题, 但是不能靠地球表面上的观测来解决的经验问题, 因为在地面上, 所有与欧几里得几何学的偏离都显然会是十分微小的. 在这个观点上, 他得到朋友们的支持, 如贝塞尔和奥尔伯斯, 而他们都是专业的天文学家. 作为科学家的高斯对此深信不疑, 但是作为数学家的高斯仍然心中稍存疑问, 而且肯定高斯从未发展起一种足以充分描述非欧几何的数学理论.

有一个从 19 世纪 20 年代早期高斯就可以利用的理论, 这就是微分几何学. 在这个学科里, 高斯最终于 1827 年发表了他的杰作:《曲面的一般研究》(*Disquisitiones Generales circa Superficies Curvas*). 他在其中说明了怎样在空间的任意曲面上描述几何学, 怎样把曲面的几何学的某些特性看作内蕴于此曲面, 而与此曲面如何嵌入 3 维空间无关. 这个理论使得高斯有可能考虑负常数曲率[III.78] 的曲面, 并且指明其上的三角形要用双曲三角学的公式来描述, 但是他到 19 世纪 40 年代才做了这件事. 如果他早就做了, 他就会发现满足场合 L 的几何学公式在这个曲面上是适用的.

然而, 一个曲面是不够的. 我们之所以接受 2 维的欧几里得几何学, 是因为它

是 3 维欧几里得几何学的简化. 所以想要人们接受一个 2 维的满足场合 L 的几何学, 就必须证明, 存在一个可以接受的 3 维的可以与场合 L 类比的几何学. 必须详细描述这样一个几何学, 并且证明它如同 3 维欧几里得几何学一样可信. 这件事高斯压根儿没有做过.

7. 波尔约和罗巴切夫斯基

发现非欧几何的荣誉归属于两个人：就是匈牙利人波尔约[VI.34] 和俄罗斯人罗巴切夫斯基[VI.31]. 他们互相独立地对这门学科作了非常相似的讨论. 特别是两人都既在 2 维情况也在 3 维情况描述了一个异于欧几里得几何学, 却有同样好的根据可以声称自己才是空间的真正的几何学. 罗巴切夫斯基的结果先在 1829 年发表在一个很少为人所知的俄罗斯刊物上, 1837 年又用法文发表, 1840 年用德文发表, 最后在 1855 年再用法文发表. 波尔约则在 1831 年把自己的论文以附录的形式发表在他父亲写的一本两卷集的几何书里面.

把他们的成就放在一起来讲最容易. 两人都以一种新奇的方式来定义平行线如下：给定一点 P 和一条直线 m, 则经过 P 的直线中, 有一些与 m 相交, 有一些则不相交. 把这两个集合分开的有两条过 P 的直线, 它们并不怎么与 m 相交, 但是这两条直线一条从 P 向右、一条向左地任意接近于 m. 它们就是图 3 上的直线 n' 和 n''. [罗巴切夫斯基就把这两条界限称为经过点 P 的对直线 m 的平行线. 这个定义见于他 1840 年写的一本小册子里. 其实, 这两条界限之间的所有直线也都经过点 P 而与直线 m 不相交].

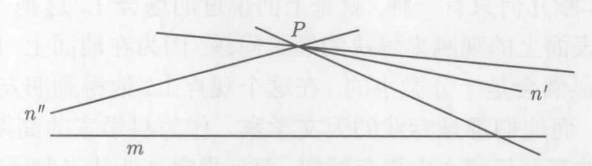


图 3 直线 n' 和 n'' 把经过 P 而与直线 m 相交或不相交的直线分离开

在这样的讨论中, 仍然可以定义从点 P 向直线 m 所作的垂线. 向左和向右的两条平行线 [即 n' 和 n''] 与这条垂线成等角, 称为平行角. 如果此角为直角, 则得欧几里得几何学. 然而, 如果它小于直角, 就有可能出现新几何学了. 结果是这个角的大小依赖于从点 P 到直线 m 的垂线的长度. 波尔约和罗巴切夫斯基都没有费心思去证明平行角小于直角不会引起矛盾. 相反, 他们都假设不会有矛盾, 然后用很大力量来从垂线的长度求平行角的大小.

他们都证明了：给定一族 (指向同一方向的) 平行线, 并在其中某一直线上指定一点, 必可经过此点作一条垂直于所有这些直线的曲线 (见图 4).

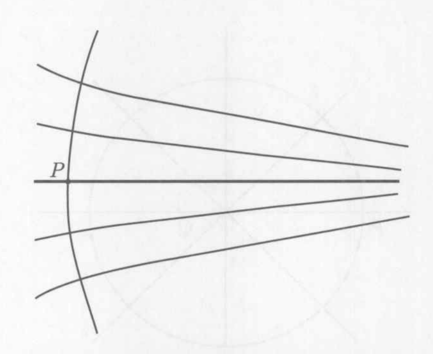


图 4 垂直于一族平行线的曲线

在欧几里得几何学中, 这条曲线是一直线, 它与族中所有平行线都垂直, 而且通过此点 (见图 5). 如果还是在欧几里得几何中, 但取一族通过公共点 Q 的直线, 并取另一点 P, 则过 P 而与所有这些直线垂直的曲线就是以 Q 为圆心并通过 P 的圆 (见图 6).

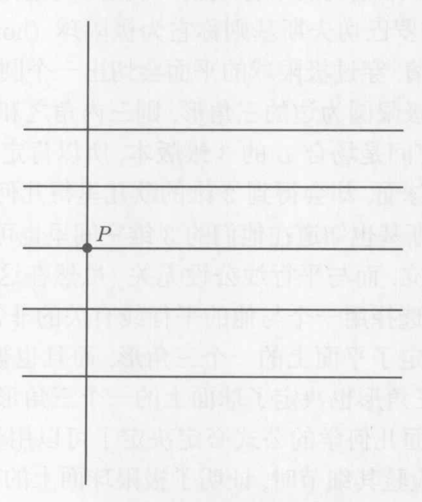


图 5 垂直于欧几里得平行线的曲线

波尔约和罗巴切夫斯基定义的这些曲线与上面两种欧几里得作图有类似之点: 它正交于所有这些平行线, 但它是弯曲的而不是直的. 波尔约称此曲线为 L 曲线, 而罗巴切夫斯基称之为极限圆 (horocycle)[①], 这个名词更有帮助, 而且一直使用至今.

①虽然中文文献中多数用了"圆"字, 极限圆却不一定是圆, 正如下面讲的"极限球"也不一定是球面一样, 要看采用非欧几何的哪一种模型而定. —— 中译本注

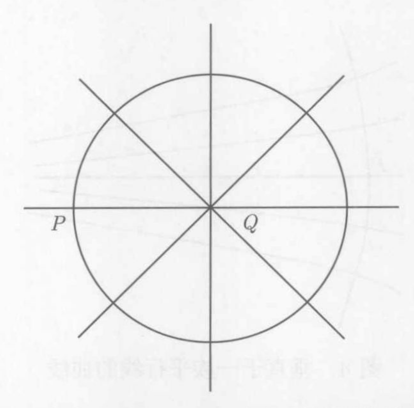


图 6 垂直于通过一点的欧几里得直线的曲线

他们的复杂论证把二人引入了 3 维几何学. 在此, 罗巴切夫斯基的论据比波尔约更清楚一点, 二人都明显超过了高斯. 如果把定义极限圆的图形绕平行线之一旋转, 这些直线就会变成 3 维空间的平行线族, 而极限圆则扫出一个杯形的曲面, 波尔约称它为 F 曲面, 而罗巴切夫斯基则称它为极限球 (horosphere). 他们都表明了会发生值得注意的事情. 穿过极限球的平面会切出一个圆, 或者切出一个极限圆, 而若在极限球面上作以极限圆为边的三角形, 则三内角之和等于两直角. 换一个说法, 虽然包含极限球的空间是场合 L 的 3 维版本, 所以肯定是非欧几里得的, 但是, 如果限制自己注意极限球面, 却会得到 2 维的欧几里得几何学!

波尔约和罗巴切夫斯基也知道在他们的 3 维空间里也可以做球, 而且证明了球面几何学的公式仍然成立, 而与平行线公设无关 (虽然在这方面, 他们不是那么有独创性). 罗巴切夫斯基选择用一个与他的平行线有关的非常聪明的做法证明了球面上的一个三角形必决定了平面上的一个三角形, 而且也被此平面三角形所决定; 反过来, 平面上的一个三角形也决定了球面上的一个三角形, 而且也被此球面三角形所决定. 这意味着球面几何学的公式必定决定了可以用于极限球面的三角形的公式. 罗巴切夫斯基在检验其细节时, 证明了极限球面上的三角形可以用双曲三角学的公式来描述, 波尔约也多少做到了这一点.

球面三角形的公式依赖于所说的球的半径. 类似地, 双曲三角形的公式也必依赖于一个实参数. 然而, 这个参数没有清晰的几何解释. 虽然有这个缺点, 这些公式有一些性质能帮助我们再次确认一些事情. 例如, 当三角形的边长很小的时候, 它们都很接近我们熟知的平面几何的公式, 这就有助于解释何以这些公式那么长时间都没有被发现 —— 它们在空间的小区域里与欧几里得几何学相差极小. 可以在这个新背景下给出长度与面积的公式, 这些公式表明三角形的面积正比于三角形的内角和与两直角之差有多少. 特别是, 罗巴切夫斯基感觉到接受这种新几何学的充分的理由在于: 有这一类干净而又可信的公式存在. 在他看来, 所有的几何学都是讲

量度的, 而各个几何定理 [的意义] 就是要把这些量度之间的可靠的联系用公式表示出来. 他的方法既然给出了这种公式, 在他看来, 作为这种新几何学存在的充分理由也就够了.

波尔约和罗巴切夫斯基既然提出了一种新奇的 3 维几何学, 于是也就提出了一个问题：哪一种几何学是真的？是欧几里得几何学, 还是其中含有参数的某个值的新几何学, 而这个参数值推测是可以通过实验来确定的？至此, 波尔约把问题丢下来就算完了, 但是罗巴切夫斯基则明确地表示, 这个问题可以通过量度星座的视差来解决. 在此, 他也没有成功, 因为这个实验是出了名的细致.

总的说来, 对于波尔约和罗巴切夫斯基的思想的反应, 在他们在世时, 就是蔑视和敌意, 他们本人也没有预见到自己的发现最终会取得的成功. 波尔约和他的父亲①把他们的工作寄给高斯. 但是高斯在 1832 年回信则说, 他不能赞扬这一工作. 因为 "赞扬它, 就是在赞扬我自己", [高斯的意思是说他本人早就得到了这样的结果], 这还不够, 高斯还加上了他对于小波尔约在文章开始处的结果给出了更简单的证明. 然而他说, 他很高兴, 因为是自己的老朋友的儿子超过了他. 小波尔约对此勃然大怒, 而且拒绝再发表自己的工作, 这样, 他就剥夺了自己通过在数学刊物上发表来保证自己的优先权的机会. 奇怪的是, 没有任何证据表明高斯事先就已知道年轻的匈牙利人的工作的细节. 很可能是高斯看到了波尔约的论著的起头就知道它下一步会怎么走.

对于现存的证据的比较宽容的解释是：在 19 世纪 30 年代, 高斯就已经相信, 物理空间有可能用非欧几何来描述, 他肯定知道怎样用双曲三角形来掌握 2 维的非欧几何 (虽然他没有留下任何详细的讨论). 但是 3 维情况首先是波尔约和罗巴切夫斯基知道, 而高斯是在读了他们的工作以后才知道的.

罗巴切夫斯基的遭遇比波尔约稍好一点. 他的最早的文章是被奥斯特罗格拉茨基 (Mikhail Vasilievich Ostrogradsky, 1801–1862, 俄罗斯数学家) 挽救了, 这是一位比他地位更高的人物, 而且是在圣 · 彼得堡的数学家, 而罗巴切夫斯基则是在外省的喀山 (Kazan, 俄罗斯的大城市, 位于伏尔加河畔). 他发表在德国的《纯粹与应用数学杂志》(*Journal für Reine und Angewandte Mathematik*, 通称 *Crelle* 杂志) 上的文章令人伤心地又多次引用了用俄文发表的文章, 此文就是由这些俄文的文章改写的. 他在 1840 年的一本小书②只得到一篇书评, 书评的愚蠢实在超过一般. 罗巴

---

①波尔约的父亲是 Bolyai Farkas. 匈牙利人的姓名的写法与中国人相似, 是姓在前, 名在后, 在欧洲这是仅有的. 所以波尔约是姓. 小波尔约名为 János (雅诺什), 但是在德文中又时常写为 Johann. 老波尔约名为 Farkas(法卡什), 用德文则作 Wolfgang. 他是高斯的老朋友, 看来在一起讨论过平行线公设一类的问题. 所以当他发现儿子在这方面有成就时, 就为儿子写信给高斯, 希望得到高斯的支持. —— 中译本注

②书名《平行线论》, 最早是用法文发表的, 2007 年又有了英译本. 值得一提的是, 此书早在 1933 年就有齐汝璜的中文译本, 收在商务印书馆的《算学小丛书》里. —— 中译本注

切夫斯基把这本小书送给了高斯, 高斯认为十分出色, 并且安排把罗巴切夫斯基选入哥廷根科学院. 但是, 高斯的热情也就到此为止, 以后罗巴切夫斯基再也没有得到过高斯的支持.

对于重大发现的如此可怕的回应, 自然引起了各个层次上的分析. 应该说, 这两人所依赖的平行线的定义, 就其实际状况来说都是不充分的, 但是对他们的工作的批评并不在此, 而是轻蔑地把他们打发了, 好像他们是不言而喻地就是错了, 错到根本不值得花功夫来找出其中一定会有的错误, 错到正当的回应就只应该是把嘲笑堆在作者头上, 或者置之不理, 不加评论. 倒是可以借此来衡量欧几里得几何学对当时的人们的思想掌控的程度, 甚至哥白尼学说和伽利略的发现, 从当时的专家那里, 也得到了更好的待遇.

8. 非欧几何被数学家接受了

当高斯于 1855 年去世后, 留下的文件中有大量未发表的数学文章, 其中就有高斯支持波尔约和罗巴切夫斯基的证据; 还有一些通信, 也认可了非欧几何可能是有效的. 当这些文件被逐步发表以后, 其效果就是使人们回来看一看波尔约和罗巴切夫斯基究竟做了些什么, 以比较正面的眼光来读一读它们.

相当偶然的是, 高斯在哥廷根有一个学生能够决定性地把事情推向前进, 哪怕实际上高斯和这位学生的接触大概还相当少. 这个人就是黎曼[VI.49]. 1854 年他被召来作就职演说答辩. 这种博士后的资格答辩是在德国大学任教的执照. 黎曼按照当时的习惯提出了三个演说题目, 而高斯作为主试人选取了黎曼最不希望的题目:《论作为几何基础的假设》. 这篇论文直到黎曼去世以后才在 1867 年发表, 它不是别的, 而是对于几何学作了完全的重新陈述.

黎曼提出, 几何学就是对他所说的流形[I.3 §§6.9, 6.10] 的研究. 这些流形是点的 "空间", 并附有距离的概念使之在小尺度上就像是欧几里得距离, 而在更大的尺度上可以大不相同. 他建议, 这种几何学可以用多种方式利用微积分来研究, 可以对任意维的流形作研究, 事实上, 黎曼甚至准备思考维数为无穷的流形.

黎曼的几何学的一个非常本质的方面就是它只研究流形的内蕴的性质, 而不问那些依赖于如何嵌入在更大的空间里的方式, 在这一方面, 他是完全遵从高斯的. 特别是, 两点 x 和 y 的距离定义为连接这两点的完全位于此曲面上的曲线的最短的距离. 这个曲线称为测地线 (在球面上, 测地线就是大圆弧).

甚至 2 维流形也各有各的不同的内蕴曲率 —— 其实, 即令单独一个 2 维流形在不同点也有不同的曲率 —— 所以黎曼的定义, 在每一个维数上, 都引导到无穷多个真正不同的几何学. 此外, 最好的是这些几何学的定义不需要参考包含它们的欧几里得空间, 所以, 欧几里得几何学的独断的地位被一劳永逸地打破了.

黎曼就职演说标题中的 "假设" 一词说明他对欧几里得所需的公设毫无兴趣.

他对于欧几里得几何学与非欧几何学的对立也没有多大兴趣. 他在这篇文章开始处只是稍稍提到, 尽管有勒让德的努力, 几何学心脏里还有一点模糊之处, 而在文章末尾, 黎曼考虑了在 2 维常曲率流形中的三种不同的几何学. 他注意到, 其中一种就是球面几何学, 另一种是欧几里得几何学, 而第三种则又不相同; 在每一种情况下, 只要知道到了一个三角形的内角和, 就可以算出所有三角形的内角和. 但是. 黎曼没有提到波尔约和罗巴切夫斯基, 只是说如果空间的几何学真是常曲率的 3 维的几何学, 则想要确定究竟是哪一种几何学, 就需要在极其广袤的区域里作量度, 而区域之大又使得这种量度是办不到的. 他讨论了把高斯的曲率推广到任意维空间, 而且指明了在常曲率空间里度量[III.56](即距离的定义) 应该是什么. 他写出的公式非常广泛, 但和波尔约以及罗巴切夫斯基的情况一样, 其中含有一个实参数 —— 即曲率. 如果曲率为负, 黎曼的距离定义就会给出非欧几何学.

1866 年黎曼去世, 而当他的就职演说发表时, 一个意大利数学家贝尔特拉米 (Eugenio Beltrami, 1835–1900) 已经独立地接近了他的某些思想. 贝尔特拉米感兴趣的是, 如果把一个曲面映为另一个曲面, 会有哪些可能性. 例如可以对一个特定的曲面 S 问, 能否找到一个映射把 S 映到平面上, 而且使每一条测地线都被映为一条直线? 他发现, 这件事当且仅当空间有常曲率时才可能. 例如从半球面到平面就有一个著名的映射具有这个性质. 贝尔特拉米找到一个简单的方法稍微修改一下公式, 使它定义一个从常负曲率曲面到圆盘内域的映射, 而且他认识到这样做的意义: 他的映射在圆盘内域定义了一个度量, 而所得的度量空间服从非欧几何的公理, 所以, 这一组公理不会导致矛盾.

其实, 在德国, 数学家明定 (Ferdinand Minding) 早几年就找到过这样一个具有常负曲率的曲面, 他称此曲面为伪球面 (pseudosphere), 是由一条称为曳物线的曲线绕自己的轴旋转而得的. 这个曲面形状像喇叭, 看来与欧几里得平面比较起来颇不自然, 很不适合作为其对手. 几年以后, 伪球面又由刘维尔[VI.39] 独立地重新发现, 而柯达齐 (Delfino Codazzi, 1824–1873, 法国数学家) 也从这个来源得知了这个曲面, 并且发现其上的三角形服从双曲三角学. 但是这些人没有一个看到它与非欧几何学的联系, 这要有待于贝尔特拉米了.

贝尔特拉米认识到, 他的圆盘描述了一个常负曲率空间, 在其中罗巴切夫斯基几何学为真 (但是贝尔特拉米不知道波尔约的工作). 他看到他的圆盘与伪球面的关系, 可以说是类似于平面与无限圆柱面的关系. 经过一段时期的怀疑以后, 贝尔特拉米学到了黎曼的思想, 而且认识到他的圆盘就是非欧几何的空间的最好不过的描述, 没有必要再去把他的几何学实现为 3 维欧几里得空间的某个曲面上的几何学. 于是, 他在 1868 年发表了自己的论文. 这是我们可以称呼为非欧几何这个数学领域的坚实基础第一次公开问世.

1871 年, 年轻的克莱因[VI.57] 也开始投身到了这个学科. 他知道英国数学家凯

莱[VI.46] 正企图把欧几里得度量引入射影几何[I.3 §6.7]. 当克莱因还在柏林学习时, 他就想要推广凯莱的思想, 把贝尔特拉米的非欧几何学也纳入射影几何学为其特例. 他的思想遭到魏尔斯特拉斯[VI.44](当时柏林的领头的数学家) 的反对, 理由是射影几何学不是度量几何学, 所以, 他宣称, 射影几何学不能产生度量概念. 但是克莱因坚持下来了, 而且在 1871–1873 三年的三篇文章里证明了所有已知的几何学都是射影几何学的子几何学. 他的思想是把几何学重新铸造成为对于作用在空间上的某个群的研究. 图形 (即空间的某个子集合) 的在此群作用下不变的性质就是几何性质. 所以, 例如对于某一维的射影空间, 适合于射影几何学的群就是所有映直线为直线的所有线性变换的群, 而其中把某一给定的圆锥映入此圆锥内域的线性变换所成的子群, 就可以看成非欧几何的变换群 (见下面的方框, 关于克莱因研究几何学的途径 [I.3 §6] 中有详细的讨论).

交比和圆锥内的距离. 平面的射影变换把同一直线上的 4 个不同点 A, B, C, D 映为另外 A', B', C', D', 而且保持

$$\frac{AB}{AD}\frac{CD}{CB}$$

不变, 即

$$\frac{AB}{AD}\frac{CD}{CB} = \frac{A'B'}{A'D'}\frac{C'D'}{C'B'}.$$

这个量称为 A, B, C, D4 点的交比, 并且记为 $CR(A, B, C, D)$.

1871 年, 克莱因把非欧几何描述为在一给定的圆锥 K 内之点的几何学, 它所允许的变换是把 K 映为自身, 内域映为内域的射影变换 (见图 7). 为了定义 K 内两点 P, Q 的距离, 克莱因注意到如果把直线 PQ 延长到与 K 相交于 A, D 两点, 这时, 交比 $CR(A, P, D, Q)$ 在射影变换下不变, 就是说, 它是一个射影不变量. 此外, 若 R 是直线 PQ 上的第三点, 而其次序为 P, Q, R, 则 $CR(A, P, D, Q)\,CR(A, Q, D, R) = CR(A, P, D, R)$. 依照此式, 克莱因定义两点 P, Q 的距离为 $d(PQ) = -\frac{1}{2}\log CR(A, P, D, Q)$(引入因子$-\frac{1}{2}$ 是为了以后引入三角学的方便). 按照这个定义, 沿一直线的距离是可加的, $d(PQ)+d(QR) = d(PR)$.

19 世纪 70 年代, 克莱因的信息是由他的上述文章中的第一和第三篇传递的. 这些文章发表在当时新创办的刊物《数学年刊》(*Mathematische Annalen*) 上. 随着克莱因名声的增长, 情况有了改变, 到 19 世纪 90 年代, 当他把第二篇文章重新发表, 而且此文又被译为几种文字以后, 使这篇文章, 即著名的埃尔朗根纲领, 广为人知. 埃尔朗根大学就是克莱因当了教授的大学, 当时克莱因非常年轻, 只有 23 岁. 但是它并不是克莱因的就职演说 (那是一篇关于数学教育的文章). 有好多年, 埃尔朗根纲领这篇文章还是奇怪地少为人知, 看来, 当时这篇文章对数学的影响并不像

有些历史学家认为的那样.

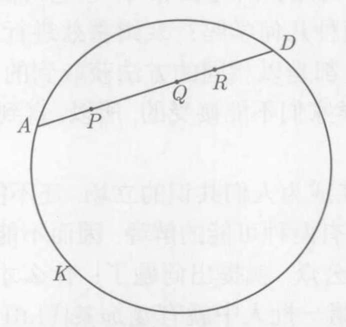


图 7 克莱因的非欧几何的射影模型中一条直线上的三点 P, Q, R

9. 还要说服其他人

非欧几何学的工作把人们的注意力从几何图形引向了那些在关键方面不改变这些图形的变换. 例如, 欧几里得几何中, 重要的变换有我们熟悉的旋转和平移 (如果您愿意的话, 还可以加上反射). 这些变换相应于刚体的运动, 而当代的心理学家认为, 人们正是通过刚体运动来认知周围的空间的. 但是这个理论在哲学上是颇有争议的, 特别是在它有可能被推广到另一种度量几何学, 即非欧几何学时也是如此. 因此, 克莱因小心地把自己的数学论文标题定为《论所谓非欧几何学》, 以安抚持敌意的哲学家们 (特别是哥廷根的很有地位的康德哲学家罗泽 (Rudolf Hermann Lotze, 1817–1881)). 但是, 克莱因的这些文章和贝尔特拉米以前的工作已经提出了充分的论据, 几乎所有的数学家都被说服了. 他们相信除了欧几里得几何学以外, 现在还有一种同样有效的数学系统, 称为非欧几何学, 至于要问哪一个在空间中是真的, 似乎非常清楚, 欧几里得几何学是明智之选, 这也没有疑问, 无需讨论了. 利普希茨 (Rudolf Otto Sigismund Lipschitz, 1832–1903, 德国数学家) 证明了可以在这个新背景下让物质就放在这里, 这样做出全部力学来, 这只是一个有某种魅力的假设的情况, 而除此以外就什么意外也没有了. 当时居于领导地位的物理学家亥姆霍兹 —— 他认识黎曼本人 —— 对此也有了兴趣, 而且写了一篇文章论述空间应该是什么样的, 才能在其中有自由的运动. 他的第一稿有大错, 因为他当时还不知道非欧几何学, 但是当贝尔特拉米向他指出错误以后, 他又写了第二稿 (1870 年). 重写的文章在数学上仍有瑕疵, 后来由李[VI.53] 向他指出. 但是, 他马上就在哲学上遇到了麻烦.

他们的问题是: "非欧几何学是一种什么样的知识?" 康德哲学正在回潮, 又成了一种时尚, 而在康德看来, 关于空间的知识是一种基本的纯粹先验的直觉, 而不是要由实验来决定的事情: 没有这种直觉, 就根本不可能有关于空间的任何知识. 面对着非欧几何这样一种对立的理论, 新康德主义哲学家遇到问题了. 他们可以同

意, 数学家们做出了一个新的冗长的逻辑练习, 但它可能是关于世界的知识吗? 难道不是肯定, 世界不会有两种几何学吗? 亥姆霍兹进行了反击, 论争说, 欧几里得几何学抑或是非欧几何学, 都是以相同的方法获取到的 —— 通过经验 —— 但是这种经验主义的调门是哲学家们不能接受的, 所以, 直到 20 世纪初叶, 非欧几何对于他们还是一个问题.

其实数学家们对于正在成为人们共识的立场, 还不能给出完全严格的辩护, 而当新闻传开, 说是对于空间有两种可能的解释, 因而不能断定欧几里得几何学一定是对的, 这时, 受过教育的公众, 就提出问题了: 什么才是空间的几何学? 按照这种新的提法来掌握问题的第一批人中就有*庞加莱*[VI.61]. 他在 19 世纪 80 年代, 由于在一系列了不起的文章中重新提出了贝尔特拉米的圆盘, 并使之成为共形的 (conformal), 而在数学上得了大名声. 所谓共形就是说非欧几何的角度和模型中的角度是相同的, 然后就用新的圆盘模型把复变函数论、线性微分方程理论、*黎曼曲面*[III.79] 和非欧几何连接起来, 生成了一个丰富的新思想的整体. 后来, 在 1891 年他又指出, 这个圆盘模型使我们能够证明非欧几何的任意矛盾必定导致欧几里得几何学里的矛盾, 反之亦然. 所以欧几里得几何学是相容的, 当且仅当非欧几何是相容的. 这件事情有一个奇怪的推论: 如果有什么人真正能从欧几里得几何的核心导出了平行线公设, 那他们必然在无意之中证明了欧几里得几何学是不相容的!

要想确定是哪一种几何学描述了真正的宇宙, 一个显然的方法是诉诸物理学. 但是庞加莱不相信这一点, 他在另外一篇文章 (1902 年) 中论证说, 对于经验可以有多种解释, 没有一种合乎逻辑的方法能够决定哪些属于数学, 哪些属于物理学. 举例来说, 设想有一种精巧的量度图形内角和的方法, 说不定是天文学尺度的图形. 这里需要取什么东西为直的, 可能是取光线为直的. 如果最终得出结论说三角形内角和小于两直角, 而且其差的大小正比于三角形面积. 庞加莱说, 这时仍然有两个可能的结论: 其一, 光线是直的, 而空间的几何学是非欧几何学; 其二, 光线是曲的, 而空间是欧几里得空间. 他接着指出, 进一步, 没有一种合乎逻辑的方法来在这两种可能性里作选择.

这种哲学立场在 20 世纪好长一段时间里以约定论 (conventionism) 之名存在着, 但在庞加莱的有生之年, 远未被人们接受. 约定论的一位著名批评者是意大利数学家恩里克斯 (Federigo Enriques, 1871–1946), 他和庞加莱一样, 既是一位强有力的数学家, 也是关于科学和哲学问题的通俗文章的作者. 他的论据是, 一个性质是几何性质还是物理性质, 可以从我们是否对它有控制而定. 我们不能改变引力定律, 但是可以通过让物质运动而改变一个质点受到的引力. 庞加莱曾经把他的圆盘比作一个金属圆盘, 使其中心很热, 而向外边运动时变冷. 他曾经给出过一个冷却定律来产生和非欧几何同样的图形. 恩里克斯回答说, 热也是可以改变的东西. 如庞加莱所应用的那种确实在我们控制之外的性质就是几何性质.

10. 展望

这个问题最终还是解决了, 但是完全不是按其自己的提法来解决的. 有两个发展把数学推动得远远超过了庞加莱的简单的二分法. 第一个是: 从 1899 年开始, 希尔伯特[VI.63] 按照公理化的途径对几何学进行了广泛的改写, 他的这项工作使得某些意大利数学家的早期思想黯然失色, 开辟了许多公理化研究的道路. 希尔伯特的工作极其出色地获得了一个思想: 如果说数学是坚固可靠的, 那么来自它的推理的本质是坚固可靠的, 这引导到数理逻辑的深刻研究. 第二个是: 爱因斯坦在 1915 年提出了广义相对论, 它在很大程度上是引力的几何理论. 对于数学的信念被恢复了, 对于几何学的感觉大为扩大了, 对于几何学和空间的关系的洞察也复杂多了. 爱因斯坦充分地应用了关于几何学的现代观念, 如果没有黎曼的工作, 爱因斯坦的成就是不可思议的. 他把引力描述为 4 维时空流形的一种曲率 (见广义相对论和爱因斯坦方程[IV.13]), 他的工作引导到关于宇宙的大尺度结构以及宇宙的最终命运的新的思考方式, 引导到至今仍未回答的问题.

进一步阅读的文献

Bonola R. 1955. *History of Non-Euclidean Geometry.* translated by Carslaw H S and with a preface by Enriques F. New York: Dover.

Euclid. 1956. *The Thirteen Books of Euclid's Elements,* 2nd edn. New York: Dover.

Gray J J. 1989. *Ideas of Space: Euclidean and Non-Euclidean Geometry and Relativistic,* 2nd edn. Oxford: Oxford University Press.

Gray J J. 2004. *Janos Bolyai, Non-Euclidean Geometry and the Nature of Space.* Cambridge, MA: Burndy Library.

Hilbert D. 1899. *Grundlagen der Geometrie* (many subsequent editions). Tenth edn., 1971, translated by Unger L. *Foundations of Geometry.* Chicago, Il: Open Court.

Poincaré H. 1891. Les géometrié non-Euclidienne. *Revue Générales des Sciences Pures et Appliquées,* 2: 769-74. Reprinted, 1952. in *Science and Hypothesis,* 35-50. New York: Dover.

—. 1902. L'expérience et le géométrie. In *La Science et l'Hypothèse,* 95-110. Reprinted, 1952, in *Science and Hypothesis,* 99: 72-88. New York: Dover.

II.3 抽象代数的发展

Karen Hunger Parshall

1. 引言

代数是什么? 对于第一次接触代数的中学生来说, 代数是 x, y, a, b 之类字母构

成的不熟悉的抽象的语言, 并有对这些符号进行操作的一些规则. 这些字母, 有的代表变量, 有的代表常量, 可以有多种用途, 例如可以利用它们来把直线写成 $y = ax+b$ 这样的形式, 可以画出它们的图像, 在笛卡儿平面上看见它们. 进一步, 还可以对这些等式进行运算和解释, 可以决定这样一些事情, 例如一条直线的根 (如果它有根的话)—— 根就是直线与 x 轴相交的地方 —— 还可以决定它的斜率是多少, 也就是它们在平面上相对于坐标系有多么陡、多么平. 有一些技术可以用来解联立方程式, 也就是决定两条直线何时相交, 又在哪里相交 (或者证明它们平行).

当似乎有许多技巧和抽象的操作来处理直线时, 其实赌注已经大为提高了. 更复杂的曲线, 例如二次曲线 $y = ax^2 + bx + c$、三次曲线 $y = ax^3 + bx^{+}cx + d$、四次曲线 $y = ax^4 + bx + cx + dx + e$ 都进入了视野, 但是同样的记号、同样的规则都还适用, 问的也是同样的问题: 一条曲线的根在哪里? 给出两条曲线, 它们在哪里相交? 如此等等.

现在还是假设中学生已经掌握了这一类代数, 进了大学, 在大学里听一门代数课, 那些他已经熟悉的 x, y, a, b 现在都不见了; 那些美丽的图像, 它们给出了一种方法, 来看出现在正在进行的事情, 基本上也不见了. 大学的课程反映的是另外一番天地, 代数不知怎么变成 “现代” 的了. 这个现代代数学讲的是抽象的结构 —— *群*[I.3 §2.1]、*环*[III.81 §1]、*域*[I.3 §2.2], 还有别的各有自己的称谓的对象 —— 每一个都是用少数几个公理来定义的, 还建立了一些子结构, 如子群、理想和子域. 在这些对象中可以通过以下映射四处游走, 如群的同态、环的*自同构*[I.3 §4.1], 等等. 这种新的代数学的目的之一是理解这些对象下面的结构而建立起群、域的完整的理论. 然后这些抽象的理论就会被应用到不同的领域里去, 在那里基本的公理是满足的, 但是事先完全看不出会有一个群或者环或者域躲在那里. 这在事实上正是现代代数学的伟大力量所在: 只要证明了一个关于某个代数结构的一般的事实, 就再也没有必要在每一次与这个结构的特例相遇时候, 再去分别指明一次这个事实. 这个抽象的途径使得我们能在看来完全不相同的背景下, 看出很重要的相似之处.

这两种事业 —— 中学里对于多项式方程的分析和大学做研究的数学家的现代代数学 —— 看起来目的如此不同, 工具和原理的展望也大异其趣, 居然都叫做 “代数学”, 这是怎么回事呢? 它们确实互有关联吗? 事实上是有的, 但是怎么会有, 这可是一篇又长又复杂的文章.

2. 有代数学以前的代数: 从巴比伦到希腊化时期

求解今天所谓的一次和二次多项式方程在古代巴比伦的楔形文字的文件中就可以找到了, 时间可以追溯到公元前 2000 年. 但是这些问题既不是用今天中学生认得出来的记号来写的, 解法也不是用的已经成了今天中学代数课程的特征的一般方法. 说这些文件提出一些特定的题目, 用一些如同秘诀一样的步骤给出特殊的解,

没有一般的理论论证, 题目大多已经改造成了几何题目, 例如量度直线段和量度具有特殊面积的曲面. 例如下面就是从藏于英国博物馆的泥砖 (编号为 BM13901, 问题 1) 上抄录翻译出来的, 其年代约为公元前 1800—1600 年①:

> *问题 1 我将以正方形的面积与边长相加得 0:45, 写下系数 1. 取 1 的一半, 0:30 自乘得 0:15, 0:15 加上 0:45 得 1, 这是 1 的平方. 1 减去自乘数②0:30, 得 0:30, 即正方形的边长.*

用现代记号, 这就是求解方程 $x^2+1x=\frac{3}{4}$. 这里要注意, 巴比伦人用的是 60 进制, 所以

$$0:45=45'=45/60=3/4.$$

同理, $0:30=30'=30/60=1/2; 0:15=15'=15/60=1/4$(见从数到数系[II.1 §1]). 然后, [记边长为 x], 泥板上的文字要求取线性项的系数 1, 把它的一半, 即 0:30 平方, [得到 0:15, 即 1/4. 再把 0:45 加进去, 这样就算出了现代记号下的 $\frac{\sqrt{b^2-4ac}}{2a}=\sqrt{\left(\frac{b}{2a}\right)^2-\frac{4ac}{4a^2}}$, 亦即 $\frac{1}{4}+\frac{3}{4}=1$ 的平方根, 但是, 1 仍为 1 的平方, 所以平方根仍为 1. 再用 $-\frac{b}{2a}$ 加进去, 亦即文中所谓减去自乘数 (本书原文没有 "自乘数" 这几个字, 而是"在得到的 0: 30 中挖掉它"), 又得到 0: 30, 即 1/2, 这就是正方形的边长 x. 现代读者容易看到这就等价于现在所称的二次方程公式, 但是巴比伦泥板就一个特定问题用文字写出了它的文本, 而对于另外的特定问题, 就要再重复一次这个文本. 这里并没有现代意义下的方程式, 巴比伦的作者们是用文字来构筑一个几何图形. 类似的问题和类似的算法解在埃及的文件如莱因德纸草书里也可以找到, 这本纸草书据信年代为公元前 1650, 而且是录自更早一个半世纪前的文本,

这种早期的文件都是以问题指向和非理论途径为特征的, 这与欧几里得[VI.2]在他的几何学杰作《几何原本》(约公元前 300 年) 中引入数学的公理化的演绎的途径形成了鲜明的对照 (关于这部书, 可在几何学[II.2] 中找到详细的讨论). 在那部书里欧几里得在显示的定义和少数几个公理或者说是自明的真理的基础上, 进而在严格几何的背景下, 导出了已知的结果 —— 但几乎可以断定还有一些迄今未知的结果, 在公理化背景下确定了欧几里得严格性的标准. 但是这种本质上是几何的文本与代数有什么关系? 考虑《几何原本》卷II的第六个命题. 这一卷表面上是讲

①由于原文很晦涩, 我们再次借用了李文林编《数学珍宝》23-24 页的译文. 这块泥砖的英译文是来自 J. Fauvel, J. Gray. *The History of Mathematics: A Reader*, 31-32. 下面的数目也相应作了一些改动. —— 中译本注

②此处《数学珍宝》的文字与本书不同, 我们要加以解释. —— 中译本注

平面图形, 特别是四边形的[①]:

> 若直线 $[AB]$ 在 $[C]$ 点平分, 在把直线 $[BD]$ 加上去, 成为直线 $[AD]$. 由整个直线 $[AB]$ 和加上去的直线 $[BD]$ 为一边, 以加上去的直线 $[BD]$ 为另一边 $[AK]$ 成一矩形 $[ADMK]$. 它与半条直线上的正方形合在一起, 等于半条直线 $[CB]$ 加上附加上的直线 $[BD]$ 上的正方形.

虽然看起来是作了一个几何作图, 它也可以同样看成是两个几何作图 —— 即一个矩形和一个正方形 —— 的面积相等. 所以, 它描述的事实应该能够写成一个方程式. 图 1 给出了欧几里得的作图的图示: 先证明了矩形 $ADMK$ 的面积等于矩形 $CDML$ 和 $HMFG$ 的面积之和, 然后再把 CB 边上的正方形, 即 $LHGE$, 分别加到矩形 $CDML$ 和 $HMFG$ 上去, 这就给出了正方形 $CDFE$. 不难看到这就等价于中学里讲的 "补成长方形的方法". 如果再令 $CB = a, BD = b$, 又看到它等价于代数等式 $(2a + b)\,b + a^2 = (a + b)^2$. 确实是等价, 但是对于欧几里得, 这是一个特定的几何作图, 一种特定的几何等价性. 由于这个 [关于几何学的] 理由, 欧几里得除了正的实量以外, 不可能处理其他对象, 而几何图形的边只可能用这种量来量度. 负的量没有进入, 也不可能进入, 欧几里得的数学天地基本上是几何的数学天地. 然而, 在历史文献中, 欧几里得的《几何原本》第二卷时常被描述为讲的是 "几何化的代数", 而且由于我们对这卷书自由地翻译为代数的语言, 可以论证, 虽然有点不符合历史, 欧几里得心里想的是代数, 不过他是把代数几何地表述出来.

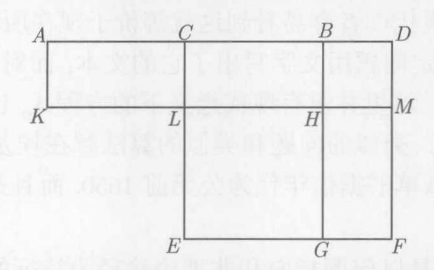


图 1　欧几里得《几何原本》卷 II 的第六个命题

虽然后来欧几里得关于严格性的几何标准被视为数学成就的一个顶峰, 但在许多方面, 它在经典的希腊古籍的数学里面并非典型的. 这方面的例子没有比阿基米德[VI.3] 更好的了, 而许多人认为在所有历史时期中, 如阿基米德这样的最伟大数学家不过三四人而已. 而阿基米德也如欧几里得一样, 是几何地提出和解决特定问题的. 当由几何学规定了严格性的标准时, 不仅负数得不到考虑, 而且我们认为是多项式方程的, 只要次数大于 3, 也基本上得不到考虑 (正如上面来自欧几里得的例子中, 二次方程式是来自补成长方形这样的几何程序, 可以设想, 三次方程式应

①我们在原书的命题文字中加上了字母, 使读者更容易看懂, 这些字母是原书没有的.—— 中译本注

该来自补成立方体的几何程序, 但是在我们熟悉的 3 维空间里, 4 次或更高次的多项式就不能这样来构造了). 然而在我们这篇数学故事里, 还有一位具有极大重要性的数学家, 就是亚历山大里亚的丢番图 (Diophantus of Alexandria), 而他在三世纪中叶是很活跃的. 他也像阿基米德一样, 提出的都是特定问题, 但是他是以一种算法风格去解决这些问题的, 比起阿基米德的几何作图方法, 更相似于老巴比伦的文本.

丢番图的名著是《算术》(*Arithmetica*) 一书, 他在其中提出了一般的不定问题, 而在给出特定的解法以前, 先要确定解应该具有特定的形式. 他对这些问题的表述与纯粹使用文字的风格大不相同, 而影响了他以后的好几个世纪. 他使用的记号也更加代数化, 最终证明对于 16 世纪的数学家 (见下文) 颇有启发. 特别是他使用了特殊的简写方式, 使他能够处理未知数的前六个正负幂以及零次幂. 这样, 他的数学再也不能是欧几里得和阿基米德那样的 “几何化的代数” 了.

例如考虑《算术》卷 II 里的一个题目: “求三个数, 使其中任一个的平方减去下一个都等于一个平方”. 用现代记号来写, 他先规定关注以下形式的解: $(x+1, 2x+1, 4x+1)$. 很容易看到 $(x+1)^2-(2x+1)=x^2, (2x+1)^2-(4x+1)=4x^2$, 所以附加条件中有两个已经满足. 但是他还要求 $(4x+1)^2-(x+1)=16x^2+7x$ 也是一个完全平方, 他就随意地令此式等于 $25x^2$, [所以就得到]$16x^2+7x=25x^2$, 丢番图由此决定取 $x=\frac{7}{9}$ 来满足这个条件. 这样他就得到了问题的一个解 $\frac{16}{9}, \frac{23}{9}, \frac{37}{9}$, 于是问题解决. 他并没有给出解法的几何论证, 因为他觉得没有必要; 他需要的就是一单个数值解. 他没有建立起我们认为是更一般的方程组, 也没有打算找出所有的解.

丢番图生活于阿基米德去世后四个世纪, 他既不研究几何学, 也不研究现代意义下的代数学, 他所提出的问题和得到的解答也和欧几里得及阿基米德大不相同. 丢番图在何种程度上是创造了一个全新的途径, 或者只是延续了亚历山大里亚可以称为 “算法化的代数” 的传统, 而与 “几何代数” 相对立, 对此学者们仍不清楚. 但是很清楚, 当丢番图的思想在 16 世纪传入拉丁西方①后, 这些思想对于长期受到几何学的权威制约的数学家们提出了新的可能性.

3. 有代数学以前的代数: 中世纪的伊斯兰世界

然而数学思想的传递是一个复杂的过程. 在罗马帝国覆灭以及学术在西方继之衰落以后, 无论是欧几里得的传统还是丢番图的传统最后都进入了中世纪的伊斯兰世界. 在那里, 这些传统 —— 通过伊斯兰学者主动的创新翻译活动 —— 不仅得

①拉丁西方与希腊东方相对立, 是指东西罗马帝国都衰落以后, 原来的希腊–罗马传统在这个大帝国的东西两部分发展很不相同. 东部的文献常用希腊文, 所以称为希腊东方, 而西部文献常用拉丁文, 所以称为拉丁西方. 本文所讲的时期, 就是文艺复兴时期, 这时老的希腊文明, 包括其数学成就从伊斯兰的东方世界传入了拉丁西方. —— 中译本注

到了保存, 还得到了进一步的研究与扩展.

阿尔 · 花拉子米[VI.5] 是巴格达的皇家建立的 “智慧宫” 里的学者. 他把欧几里得的《几何原本》第二卷里面所讲的几何论证, 和可以追溯到古代巴比伦的精巧的解题算法连接了起来. 特别是, 他写了一本关于实用数学的书, 现在简称为《代数学》, 而其原来的书名则是 *al-Kitāb al-mukhatasar fī hisab al-jabr wa'l-muqābala* (《通过补全和还原作计算的纲要》), 其中的 al-jabr[就是 “还原” 也就是现在说的 “移项”] 一词, 拉丁化以后就是现代名词的 algebra, 也就是 “代数学”. 因为他不使用负系数和零系数, 所以就把现在只需归为一类 $ax^2+bx+c=0$ 的二次方程式, 分成了六类. 例如, 他考虑了所谓 “平方和根等于数” 的一类的一个例子①: “一个平方和十个根等于三十九”, 他的用乘法、加法和减法来表示的算法解恰好与上面所说的泥砖 BM13901 上的解法完全一样. 然而, 对于阿尔 · 花拉子米, 这还不够, 他说: “我们还必须用几何来证明这个问题的 [解法] 是真理, 而同是这个问题, 我们已经用数来解决了”, 然后他就接着用几何方法来 “补足正方形”, 很像欧几里得在《几何原本》第二卷中所做的那样, 不过没有那么形式化 (Abū Kāmil (约公元 850–930), 一位比阿尔 · 花拉子米晚了大约一代人的埃及伊斯兰数学家, 在几何 — 算法背景下, 引入了更高水平的欧几里得形式化). 这样把二者并列使得几何学里的面积和直线的关系可以用数值的乘法、加法和减法显示地表现出来, 这一关键的步骤终于提示了从特殊问题的几何解法转向一般类型的方程式的代数解法.

奥马尔 · 哈亚姆 (Omar Khayyam, 约公元 1050–1130), 一位数学家和诗人, 在这条路上走了另外一步. 他写了一部书, 书名仿照阿尔 · 花拉子米的书, 也叫《代数学》(*Al-jabr*), 在书中他系统化地解决了我们现在认识到是三次方程式的问题, 但是是在没有负系数和零系数的情况下. 哈亚姆也仿照阿尔 · 花拉子米给出了几何论证, 但是他的著作更甚于他的前人, 可以看作是对于特定问题的一般解题技术, 也就是更接近代数概念.

波斯数学家 al-Karajī (他在公元 11 世纪中叶很活跃) 对于来自欧几里得《几何原本》的几何传统也很喜爱并且熟悉. 然而, 他也像 Abū Kāmil 一样, 也知道丢番图的传统, 而且在比较一般的背景下综合了丢番图在《算术》中给出的特殊例子. 虽然这个或那个中世纪的伊斯兰数学家都知道丢番图的思想和风格, 拉丁西方的数学家在 16 世纪重新发现他们, 并翻译他们的著作以后才知道他们. 印度数学家的成就同样也是拉丁西方所不知的, 他们在八世纪初就已经算法地解出了某些二次方程式, 而如婆罗摩笈多 (Bragmagupta, 598–670, 印度数学家) 以后 400 年, 又知道了我们今天称为佩尔 (Pell) 方程的某些特例的整数解的方法, 所谓佩尔方程就是形如 $ax^2+b=y^2$ 的方程, 其中 a, b 是整数, 但 a 不是完全平方.

①这个例子见于该书第四章: “平方和根等于数”. 这里的译文借用了李文林《数学珍宝》99 页. —— 中译本注

4. 有代数学以前的代数：拉丁西方

与伊斯兰在东方兴起的同时, 拉丁西方在罗马帝国衰落后的几个世纪里也在经历逐渐的文化和政治的稳定过程. 到了 13 世纪, 相对的稳定导致了天主教廷的巩固, 还有大学和活跃的经济的建立. 到 8 世纪, 伊斯兰征服了伊比利亚半岛[①], 后来在那里建立了伊斯兰的宫廷、图书馆和类似巴格达的智慧宫那样的研究机构, 把中世纪的伊斯兰的学术带到了欧洲大门口. 到了 12 和 13 世纪, 当伊斯兰感觉到自己在伊比利亚半岛的地位已经岌岌可危的时候, 伊斯兰的学术成就, 以及由伊斯兰学者们译为拉丁文而保存下来的希腊学术成就, 已经渗入中世纪的欧洲了. 特别是斐波那契[VI.6], 比萨城邦一位有影响的官员的儿子, 读到了阿尔 · 花拉子米的著作, 不仅认识到其中详细说明的阿拉伯记数系统可以对会计和商业有用 (当时广泛使用的还是罗马数字及其繁琐的运算规则), 也认识到阿尔 · 花拉子米的理论讨论的重要性, 包括认识到我们可以解释为一次和二次方程式的几何证明与算法求解的联姻. 在他著于 1202 年的《算经》(*Liber Abbaci*) 一书里, 斐波那契几乎是逐字陈述了阿尔 · 花拉子米的工作, 赞扬其种种优点, 这样就把这种知识和方法传入了拉丁西方.

斐波那契对于阿尔 · 花拉子米的书, 特别是起实用的部分的介绍, 很快就在欧洲流行开了. 所谓的 "abacus" 学校 (这里的 abacus 一字是指斐波那契的《算经》一书, 而不是中国的计算工具算盘, [珠算算盘英文也是 abacus]) 在意大利半岛上兴起如雨后春笋, 特别是在 14 和 15 世纪, 目的是为了日益商业化的西方世界训练会计和簿记人员. 这些学校的教员, 就是所谓 "abacus 师傅" (maestri d'abaco) 都是依赖在斐波那契的书中找到的算法, 并且加以发展. 另一个传统, 所谓 Coss 传统 (Coss 是一个德文词, "有技巧的计算", 意味着代数), 则在欧洲的日耳曼地区同时发展起来, 目的在于把代数引入那里的主流.

1494 年, 意大利数学家帕乔利 (Luca Bartholomeo de Pacioli, 1445–1717) 写了一本书 (现在, "帕乔利的书" 已经成了最为关键的词: 这本教材是最早的印刷出版的数学教科书之一), 它是所有当时已知数学知识的概览, [全名 *Summa de Arithmetica, Geometria, Proportioni et Proportionalita* (以下简称 *Summa*, 即《概要》, 它在意大利北部广为流传, 而且还包含了威尼斯商人们在文艺复兴时期所用的会计系统, 帕乔利也被称为 "会计学之父"). 到了那时, 阿尔 · 花拉子米和斐波那契所陈述的几何论证, 在意大利本国语言中早已没有了. 帕乔利的《概要》, [由于是第一本印刷出版的用意大利口头语写的教本], 就把这种几何论证重新推上了数学的前台. 帕乔

①伊比利亚半岛就是欧洲西南部的半岛, 西临大西洋和比斯开湾, 东接地中海, 南隔直布罗陀海峡与非洲相望, 北以比利牛斯山脉为界连接现在的法国, 也就是现在的西班牙与葡萄牙. 自 8 世纪伊斯兰征服伊比利亚半岛以来, 他们和原来的统治者的矛盾一直不断, 到 16 世纪以后, 欧洲人又把伊斯兰的力量逐出了伊比利亚半岛, 所以正文中说到他们感到 "岌岌可危". —— 中译本注

利不知道奥马尔 · 哈亚姆的著作, 还说 [二次方程式] 中只发现了阿尔 · 花拉子米和斐波那契所研究过的六种特殊情况, 书中还讲到三次方程式的求解, 虽然当时这个企图流产了, 帕乔利仍然坚持最终都是有希望解决的.

帕乔利的书还突出了一个关键的未解决的问题：对于各种三次方程式能否找到算法解法? 如果可以, 对这些算法解法能否几何地加以论证, 而且得到实质上类似于在阿尔 · 花拉子米和斐波那契的教材中的那些证明?

在好几位最终肯定地回答了第一个问题的 16 世纪意大利数学家中, 就有卡尔达诺[VI.7]. 他在 1545 年出版的《大术》(*Ars Magna*) 一书, 对于各种三次方程式提出了算法解法及其几何论证, 在阿尔 · 花拉子米和斐波那契 "补足了正方形" 的地方, 有效地 "补足了立方体", 他也提出了由他的学生费拉里 (Ludovico Ferrari, 1522–1565) 发现的四次方程式的算法解法. 这些解法使他感到困惑, 因为没有几何的论证. 他在自己的书中写道："所有这一切, 直至三次方程式在内, 都得到了完全的证明. 但是其他我们想要加上的, 或者出于不得已, 或者出于好奇心, 我们还只能提出来". 代数学在打破它孕育于其中的几何的蛋壳.

5. 代数学诞生了

丢番图的《算术》在 16 世纪 60 年代被译为拉丁文, 带来了它的简洁的风格和非几何的方法, 加速了这个过程. 代数, 作为一种一般的解题的技巧, 可以应用于具有几何、数论和其他数学分支背景的问题, 是在几本书里建立起来的, 这里有庞贝里[VI.8]1572 年的《代数》一书, 特别是维特[VI.9]1591 年的《分析的艺术引论》(*Artem Anaticeum Isagoge*) 一书. 这一本书的目的, 用维特的话来说, 就是 "不留下任何没有解决的问题", 而为此目的, 他发展了真正的记号 —— 用元音字母表示变数, 而用辅音字母表示系数 —— 还有解一个未知数的方程式的方法, 他把他的技巧称为 "美丽非凡的算术运算".

然而, 维数 —— 表现为所谓**齐次性定律**—— 对于维特仍旧是一个问题. 按照他的说法："只有齐次的量才可以互相比较". 问题在于他区别了两种量："阶梯量", 即 (A 边)(用现在的记号就是 x)、(A 方)(用现在的记号就是 x^2)、(A 体)(用现在的记号就是 x^3), 还有 "比较量", 就是系数, 有一维的 (B 长度)、二维的 (B 平面)、三维的 (B 立体) 等等. 然后, 按照齐次性定律, 维特可以合法地写出 (A 体)+(B 平面)(A 边)(用现在的记号就是 x^3+bx). 因为 (A 体) 的维数是 3, 二维系数 (B 平面) 的维数是 2, 一维变数 (A 边) 是 1, 所以其乘积的维数也是 3. 但是他不能合法地把三维变数 (A 体) 和一维系数 (B 长度) 与一维变数 (A 边) 的二维乘积相加 (而在现在的记号下, 它仍是 x^3+bx). 尽管如此, 他的《分析艺术》这本书仍然准许他把字母与特定的数相对立来相加、相减、相乘和相除, 而字母只要满足齐次性定律就可以作二次、三次、四次, 实际上是任意次的幂. 他有了一个初步的代数, 但是

未能用之于曲线.

最先做到这一点的数学家是费马[VI.12] 和笛卡儿[VI.11]. 他们互相独立地发展的解析几何, 对于今天学代数的中学生如此熟悉. 费马和英国人哈里奥特 (Thomas Harriot, 1560–1621 英国数学家和天文学家) 的工作受到维特的影响, 而笛卡儿不仅引入了我们今天的记号规约, 即用 x, y, z 表示变量, 用 a, b, c 表示常数, 而且开始把代数算术化. 他引进了一个单位, 这就使他可以把所有几何量都解释为直线段, 不管是 x, x^2, x^3, x^4, 以至于 x 的任意次幂, 都是直线段, 这样他就消除了对于齐次性的担心. 费马在这个方向的主要工作是他用拉丁文写于 1636 年的一篇手稿, 题为 "论平面和立体的轨迹", 这篇手稿只在 17 世纪初在他的数学朋友们中间流传; 笛卡儿的主要著作《几何学》(*La Géométrie*) 则是他的哲学著作《方法论》(*Discours de la Méthode*) 的三个附录之一, 出版于 1637 年. 这两部著作都被认为是确定了几何曲线与二未知数的方程的同一性, 或者换句话说就是建立了解析几何, 从而把代数方法引用来解决以往认为是几何的问题. 在费马的情况, 这些曲线是直线和圆锥截线 —— 总之是 x 和 y 的二次式; 笛卡儿也这样做了, 但是他还更为一般地考虑了方程式, 抓住了多项式方程的根的问题, 这与多项式的变换和化简有关.

特别是, 笛卡儿对于我们现在所说的代数的基本定理[V.13] 已经有了一个初步的版本, 虽然他没有给出证明, 甚至没有给出一般的陈述. 这个定理说, n 次多项式方程 $x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ 在复数域中恰好有 n 个根. 例如, 他一方面坚持, 一个给定的 n 次多项式可以分解为 n 个线性因子, 同时他也认识到, 三次方程式 $x^3 - 6x^2 + 13x - 10 = 0$ 有 3 个根: 一个实根 2, 还有两个复根. 当他进一步探讨这个问题时, 还发展了包含适当的变换的代数技巧来分析 5 次和 6 次多项式方程. 笛卡儿既然已经摆脱了对于齐次性的担心, 就可以自由地用他的代数技巧来探讨倾向于几何的卡尔达诺很明显难以涉足的领域. 牛顿[VI.14] 在 1707 年他的《万有算术》(*Arithmeica Universalis*) 一书里, 在把代数从几何的担心中解放出来的方向上又向前走了一步, 论证代数的完全算术化, 以实数和通常的算术运算作为代数的模型.

笛卡儿的《几何学》至少突出了两个问题供代数作进一步探讨, 即代数的基本定理和四次以上的多项式方程式的解法. 虽然 18 世纪的数学家如达朗贝尔[VI.20] 和欧拉[VI.19] 都企图证明代数的基本定理, 但是给出严格证明的第一人是高斯[VI.26], 他在一生中共给出了四种不同的证明. 第一个是一个代数几何证明, 出现在他 1799 年的博士论文中, 而第二个证明与此不同, 发表在 1816 年, 而用现代术语来说, 本质地涉及构作多项式的分裂域. 代数的基本定理确定了一个给定的多项式方程有多少个根, 但是对于这些根确切地是什么, 又如何精确地把它们找出来, 这个定理没有提出任何见解. 那个问题和它的种种数学变形, 在 18 世纪晚期和 19 世纪激发了许多数学家, 而且最终成为在 20 世纪初形成现代代数学的几条数学线索之一. [来自代数的基本定理的] 另一股数学潮流来自企图理解 (一个或多个)n 个

未知数的多项式组的一般性态, 还有一个潮流则来自用代数方法研究数论问题的努力.

6. 寻求代数方程的根

求多项式方程的根的问题, 提供了一个连接中学教学与做研究的数学家的一个直接联系. 今天的中学生们都要按照规矩使用二次方程的公式来计算二次方程式的根. 为了导出这个公式, 我们需要把已给的方程变换成比较容易求解的形式. 卡尔达诺和费拉里对于三次和四次方程也通过比较复杂的操作得到了根的公式. 自然要问对于更高次的多项式方程能不能也这样做? 更准确地说, 有没有一个求根的公式, 其中只含有通常的算术运算 —— 加、减、乘、除以及开方? 如果有这样的公式, 就说这个方程可以用根式求解.

虽然 18 世纪的许多数学家 (包括欧拉、范德蒙德 (Alexandre-Théophile Vandermonde, 1735–1796, 法国人, 原来是音乐家和化学家, 但是主要贡献在数学)、华林[VI.21]、贝祖 (Étienne Bézout, 1730–1783, 法国数学家)) 都对于能否用根式解更高次的多项式方程做过努力, 但是直到大约 1770–1830 年间才有了显著的突破, 特别是在拉格朗日[VI.22]、阿贝尔[VI.33] 和高斯的工作中.

拉格朗日在 1771 年发表的一组很长的论文《对于方程的代数解法思考》(*Réflections sur la resolution algébrique des equations*) 中, 试图通过详细分析三次和四次方程的特例, 来决定代数方程解法下面是否有深层的一般原理. 拉格朗日以卡尔达诺的工作为基础, 证明了一个形如 $x^3+ax^2+bx+c=0$ 的三次方程总可以通过一个变换来消除其中的平方项, 成为 $x^3+px+q=0$, 而且其根可以写成 $x=u+v, u^3, v^3$ 是某个二次方程之根. 然后拉格朗日就可以证明, 如果 x_1, x_2, x_3 是这个三次方程的三个根, 则中介的函数 u, v 可以写成

$$u=\frac{1}{3}\left(x_1+\alpha x_2+\alpha^2 x_3\right), \quad v=\frac{1}{3}\left(x_1+\alpha^2 x_2+\alpha x_3\right),$$

其中的 α 是一个三次单位原根. 这就是说, u, v 可以写成 x_1, x_2, x_3 的有理表达式, 或称为预解式. 反过来, 如果从 x_1, x_2, x_3 的一个线性表达式 $y=Ax_1+Bx_2+Cx_3$ 开始, 然后让 x_1, x_2, x_3 作任意的排列得到 6 个表达式, 其每一个都是一个 6 次方程的根, 分析这个 6 次方程 (利用多项式的对称性质), 就会再次得到上面 u, v 的表达式. 拉格朗日指出, 像这样的向两端分析 —— 涉及中介的表达式, 这些表达式又都是一个可解的方程之根, 同时也涉及某个有理表达式在根的排列下的动态 —— 这样做, 在三次和四次两种情况下都会给出完全的解. 即同样一种途径, 给出了**两类**方程的解答. 但是这个方法可否推广到五次和更高次多项式呢? 拉格朗日未能把它推进到 5 次情况, 但是以他的思想为基础, 首先是他的学生鲁菲尼 (Paolo Ruffini, 1765–1822, 意大利数学家) 在 18 与 19 世纪之交 [怀疑 5 次方程其实不可能用根式

来解], 然后是年轻的挪威数学家阿贝尔, 在 19 世纪 20 年代, 确定地证明了 5 次方程确实不能用根式来解 (见五次方程的不可解性[V.21]). 这个反面的结果仍然留下一个未解决的问题: 哪些代数方程可以用根式来解, 为什么.

拉格朗日的分析似乎是强调了一点: 这个问题在 3 次和 4 次方程的情况下的解决, 关键性地分别依赖于 3 次和 4 次单位根. 由单位根的定义, 也就是依赖于特别简单的多项式方程 $x^3-1=0, x^4-1=0$. 所以很自然地会去检验一般的所谓分圆方程式 $x^n-1=0$, 并且考虑对于哪些 n, n 次单位根是可以实际构作出来的. 这个问题用等价的代数语言来表述就是: 对于哪些 n, n 次单位根可以对整数通过通常的算术运算和开平方 (但不开更高次方) 表示出来? 这是高斯在他的涵盖广泛的奠基性的杰作, 即 1802 年的《算术研究》(*Disquisitiones Arithmeticae*) 里所讨论的许多问题之一. 他最著名的结果之一就是正 17 边形 [可以用圆规和直尺] 作出来 (也就是 17 次单位根可以构作出来). 在他的分析过程中, 不但使用了类似于拉格朗日所发展出来的技巧, 还发展了一些关键性的概念, 例如模算术[III.58] 和 p 为素数时的 "模世界"$\mathbf{Z}_p$、更一般的 $\mathbf{Z}_n, n\in\mathbf{Z}^+$, 以及后来称为循环群的本原元素 (即生成元) 的概念.

大约 1830 年左右, 伽罗瓦[VI.41] 从拉格朗日关于预解式的分析和柯西[VI.29] 关于排列和代换的工作得到了多项式方程可用根式求解这个一般问题的答案, 然而我们并不清楚伽罗瓦在多大程度上也熟悉高斯的工作. 虽然伽罗瓦的工作借用了早前的思想, 但是在一个重要的方面, 它基本上是全新的. 前人的努力是朝向计算次数一定的多项式方程的根的显式的算法, 伽罗瓦则提出了一个理论程序, 使得他能够评定出一个方程是否可解, 而这种程序是从给定的方程导出的, 但是更为一般.

更详细一点来说, 伽罗瓦用了两个新的概念重新改造了这个问题. 这两个概念就是: 域 (伽罗瓦称之为 "有理性的区域") 和群 (准确一点说是置换群). 如果一个 n 次多项式方程 $f(x)=0$ 的 n 个根都在它的有理性区域 —— 其系数就来自这个域, 我们称之为基域 —— 就说这个方程在此基域上是可约的; 反之则说它在此域上是不可约的. 然而, 它可能在一个较大的域上是可约的. 例如, 考虑多项式 x^2+1 作为 $\mathbf{R}$ 上的多项式. 我们从中学代数里就知道, 它不能分解为两个实线性因子的乘积 (即不存在实数 r_1 和 r_2 使得 $x^2+1=(x-r_1)(x-r_2)$), 但是它在复数域上则可以分解, 具体说, 有 $x^2+1=(x+\sqrt{-1})(x-\sqrt{-1})$. 所以如果考虑所有形如 $a+b\sqrt{-1}$ 的数, 其中 $a,b\in\mathbf{R}$, 就会得到一个较大的域 $\mathbf{C}$, 使得多项式 x^2+1 在其上是可约的. 如果 $\mathbf{F}$ 是一个域, 而 $x\in\mathbf{F}$ 在其中不能开 n 次方, 则利用一个类似的过程, 可以把一个元 y 添加到 $\mathbf{F}$ 中去, 这个 y 要规定适合 $y^n=x$, 称为一个根式. 添加以后就得到一个新域, 比原来的 $\mathbf{F}$ 更大. 伽罗瓦证明了如果可以通过添加根式, 而逐次地把 $\mathbf{F}$ 扩大为一个域 $\mathbf{K}$, 使得 $f(x)$ 可以在 $\mathbf{K}$ 中分解为 n 个线性因子, 则 $f(x)=0$ 可以用根式解出. 他发展了一个程序, 其中有两个关键点: 一是把

一个元素 —— 特别是一个所谓的本原元素 —— 附加到基域上去的概念; 二是分析这个新的扩大了的域的内部结构, 就是分析所有这样的代换, 使得 $f(x)=0$ 的 n 个根的有理表达式不变, 这些代换 (即 $\mathbf{K}$ 的自同构) 形成一个 (有限) 群, 而伽罗瓦就是对这个群进行分析, 伽罗瓦的分析的这个群论的侧面特别具有潜力. 他引进了一些概念, 虽然用的不是当今的名词. 例如群的正规子群、因子群、可解群等等. 这样, 伽罗瓦就从群及其内部结构这个抽象的视野, 解决了多项式方程何时可以用根式求解这个具体的问题.

伽罗瓦的思想, 虽然是在 19 世纪 30 年代早期就概括地提出了, 但是迟迟没有引起更广大的数学界的注意, 直到 1846 年才在刘维尔[VI.39] 的《纯粹与应用数学杂志》(*Journalde Mathé matiques Pures et Appliquées*) 上发表, 但没有得到充分的理解, 直到 20 年后首先在塞雷特 (Joseph Alfred Serret) (1819–1895, 法国数学家) 的《高等代数教程》(*Cours d'Algébre Supérieure*, 1849), 更进一步在约当[VI.52] 的《论代换和代数方程》(*Traité des Subtitutiones et des Équations Algébriques*, 1870)①这两部教材中得到了进一步的阐述. 特别是后一本书, 不仅突出了伽罗瓦在求解代数方程上的工作, 还把置换群的理论沿着它在拉格朗日、高斯、柯西、伽罗瓦等手上的发展道路, 展开了其一般的结构理论. 到了 19 世纪末, 群论的发展线索, 原来是来自用根式求解代数方程的努力, 现在与来自其他三个方面的努力组合在一起了. 这三个方面就是: 第一, 用乘法表来定义的群的抽象概念, 这是由凯莱[VI.46] 提出的; 第二, 例如西罗 (Peter Ludwig Mejdell Sylow, 1832–1918, 挪威数学家)、赫尔德 (Otto Ludwig Hölder, 1859–1937, 德国数学家) 所做的关于结构的工作; 第三, 李[VI.53] 和克莱因[VI.57] 几何方面的工作. 到了 1893 年, 韦伯 (Heinrich Martin Weber, 1842–1914, 德国数学家) 把这些早期的工作汇编起来给出了第一个关于群和域这两个概念真正的抽象定义, 这样就把它们重新铸造成为现代数学家们熟悉得多的形式, 这以后群和域已经在极为广泛的数学和物理领域中有了中心的重要性.

7. 探讨 n 个未知数多项式的性态

求解代数方程的根的问题, 是求解含有 1 个未知数的多项式方程. 然而, 早在 17 世纪后期, 像莱布尼兹[VI.15] 这样的数学家就开始关心求解含两个以上未知数的联立的线性方程组的技巧了. 但是他的工作不为当时的人所知, 莱布尼兹考虑了含有 3 个未知数的 3 个线性方程, 并且以系数的一个特殊表达式的值来决定其可解性. 这个表达式就等价于柯西后来称的行列式 [III.15], 而且最终与系数的一个 $n\times n$ 正方形的阵列, 即矩阵[I.3 §4.2] 联系起来. 这些工作在 18 世纪中期也由克拉默 (Gabriel Cramer, 1704–1752, 瑞士数学家) 在求解含 n 个未知数的 n 个线性方程

①作者在这里给出了当年在推广群论上起了最大作用的两部教材, 后一部影响更大一些. —— 中译本注

这个一般背景下独立地完成. 行列式理论, 很快地就从这些起源独立于求解线性方程组的背景, 自身变成了代数研究的主题, 吸引了诸如范德蒙德、拉普拉斯[VI.23]和柯西这样的人的注意. 这样, 行列式就成了新代数结构的一个例子, 它的性质也被系统地研究了.

虽然行列式是被从矩阵角度来研究的, 但矩阵本身及其名称却是由西尔维斯特[VI.42] 提出的, 其理论本身最初并不是始自求解线性联立方程, 而是来自对含有两个、三个以至一般的 n 个变元的齐次多项式作变元的线性变换而来的. 例如高斯在《算术研究》里面就考虑了具有整数系数的二元、三元的二次型 —— 即 $a_1x^2+2a_2xy+a_3y^2$ 和 $a_1x^2+a_2y^2+a_3z^2+2a_4xy+2a_5xz+2a_6yz$ 这样的表达式 —— 怎样受到变元的线性变换的影响. 在三元形式情况下, 高斯作了 3 个 2 变量的线性变换 $x=\alpha x'+\beta y'+\gamma z', y=\alpha' x'+\beta' y'+\gamma' z'$, 以及 $z=\alpha'' x'+\beta'' y'+\gamma'' z'$, 并且把这个变换的系数排成一个正方形的阵列

$$\begin{matrix} \alpha, & \beta, & \gamma \\ \alpha', & \beta', & \gamma' \\ \alpha'', & \beta'', & \gamma'' \end{matrix}$$

而且在表明两个变换的复合是什么的过程中, 显式地给出了矩阵乘法法则的例子. 到 19 世纪中叶, 凯莱开始研究矩阵本身, 研究矩阵的理论作为一个数学系统本身就具有的性质. 这样的思路最终被用代数理论 (见下文 [本文 §8 末尾]) 来重新加以解释, 发展成为线性代数和向量空间[I.3 §2.3] 理论的独立的篇章.

另一个从分析齐次多项式作线性变换而出现的理论是不变式理论, 而这也是由高斯的《算术研究》开端的. 和他研究三元二次型的情况一样, 他也对二元的二次型作线性变换 $x=\alpha x'+\beta y', y=\gamma x'+\delta y'$, 结果得到一个新的二元形式 $a_1'(x')^2+2a_2'x'y'+a_3'(y')^2$, 而 $a_1'=a_1\alpha^2+2a_2\alpha\gamma+a_3\gamma^2, a_2'=a_1\alpha\beta+a_2(\alpha\delta+\beta\gamma)+a_3\gamma\delta, a_3'=a_1\beta^2+2a_2\beta\delta+a_3\delta^2$. 高斯注意到, 如果把第二个式子平方, 再减去第一、第三两个式子的乘积就会得到关系式 $a_2'^2-a_1'a_3'=(a_2^2-a_1a_3)(\alpha\delta-\beta\gamma)^2$. 如果用西尔维斯特在 19 世纪 50 年代早期发展起来的语言来说, 高斯已经认识到原来的二元二次型的系数的表达式 $a_2^2-a_1a_3$ 是一个不变式. 意即在上述线性变换下, 它的值除了增加了变换行列式的幂以外, 并未变化. 当西尔维斯特造出这个名词的时候, 不变这个现象也出现在英国数学家布尔[VI.43] 的工作中, 而引起了凯莱的注意. 但是一直到凯莱和西尔维斯特在 19 世纪 40 年代晚期在伦敦相遇以后, 他们才开始追随不变式理论本身, 其目的是找出一个含有 n 个未知数的 m 次齐次多项式的所有不变式, 以及多个这种多项式的同时的不变式.

虽然凯莱 (特别是西尔维斯特) 是从纯代数观点来追随这条研究路线的, 不变式理论在数论和几何学方面也有意义, 前者有艾森斯坦 (Ferdinand Gotthold Max Eisenstein, 1823–1852, 德国数学家) 和厄尔米特[VI.47]; 后者则有奥托 · 哈塞 (Lud-

wig Otto Hesse, 1811–1874, 德国数学家)、哥尔丹 (Paul Albert Gordan, 1837–1912, 德国数学家) 和克莱布什 (Rudolph Friedrich lfred Clebsch, 1833–1872, 德国数学家) 等人. 特别有趣的是去了解与一个特定的形式或一组特定的形式相关的到底有多少个 "真正不同的" 不变式. 1868 年, 哥尔丹取得了重要突破, 证明了 [任意二元形式的所有不变式① 都可以用其中有限多个表示出来. 但是, 当他开始考虑更多元形式时, 终因计算太繁而失败]. 然而, 到了 19 世纪 80 年代末 90 年代初, 希尔伯特[VI.63] 引入了新的抽象的与代数理论相关的新概念 (见下文 [本文 §8 末尾]), 不仅重新证明了哥尔丹的结果, 而且也证明了这个结果 [(时常称为 "有限性定理")] 对于任意多的 n 个未知数的任意高 m 次齐次多项式都是成立的. 由于希尔伯特的这项工作, 研究的重点就从他的英国和德国前人的重在具体计算转到指向结构的存在定理, 这很快就与抽象的现代代数联系起来了.

8. 寻求对于 "数" 的性质的理解

早至公元前 6 世纪, 毕达哥拉斯学派就已经从形式角度去研究过数的性质. 例如, 他们定义了完全数的概念, 即等于自己的所有因子 (除此数本身以外) 之和的正整数, 例如 $6 = 1 + 2 + 3$, $28 = 1 + 2 + 4 + 7 + 14$. 到了 16 世纪卡尔达诺和庞贝里都很乐意地去研究一种新的形如 $a + \sqrt{-b}$ 的表达式, 其中 a, b 是实数, 而且探讨了它们的计算性质. 到 17 世纪, 费马高调宣称他能够证明当 n 为大于 2 的正整数时, 方程 $x^n + y^n = z^n$ 没有整数解, 例外是 $z = x$ 或 y, 而另一未知数为零. 后一结果称为费马大定理[V.10], 产生过许多新思想, 特别是在 18 和 19 世纪当人们试图证明费马所声称的结果确实为真时. 他们的努力的核心思想是生成新的数系并从代数上去研究它们. 这些数系之推广整数的概念和伽罗瓦对于域的推广非常相似. 这种生成和分析新数系的灵活性, 当代数学进入 20 世纪时, 将要成为现代代数学的特点.

第一个冒险沿着这条道路前进的人是欧拉. 当他证明 $n = 3$ 时的费马大定理时 (这个证明见于欧拉 1770 年写的《代数学原理》一书), 引进了形如 $a + b\sqrt{-3}$ 的数所或的数系, 其中 a, b 是整数. 然后他就高高兴兴地把它们分解为素因子, 和分解普通的整数一样, 而不作进一步的论证. 到了 19 世纪二三十年代, 高斯对于现在称为**高斯整数**的数系进行了比较系统的研究. 高斯整数就是形如 $a + b\sqrt{-1}$ 的数, 其中 a, b 是整数. 他证明了高斯整数和普通的整数一样, 在加、减、乘下面都是封闭的; 他定义了单位元、素数和范数等概念, 以便对于它们证明算术的基本定理[V.14] 仍成立. 这样他就证实了还有完整的新的代数世界等待人们去创造和探

①原书作 "any binary form in n variables", 似乎有笔误, 因为 binary form 按定义就只有两个变元, 所以这里的 "n variables" 应为 "arbitary degree n" 之误 · 哥尔丹研究不变式理论的经过是数学史上有名的事例, 所以我们在此作了更正.—— 中译本注

索 (关于这个主题, 在条目代数数[IV.1] 中有详细的介绍).

欧拉是受到了他在费马大定理方面的工作的推动, 而高斯则是试图把二次互反律[V.28] 推广为双二次互反律. 在二次的情况下, 问题是: 若 a 和 m 都是整数, 而 $m \geqslant 2$, 我们说 a 是一个平方剩余 $\bmod m$, 如果方程 $x^2 = a$ 有一个解 $\bmod m$ 存在, 也就是说, 存在一个整数 x 使得 $x^2 \equiv a \bmod m$. 现在设 p, q 是互异的奇素数. 如果知道 p 是否平方剩余 $\bmod q$, 是否有一个简单的方法来说出 q 是否也是一个平方剩余 $\bmod p$? 勒让德在 1785 年提出并且回答了这个问题: 如果 p 和 q 都是同余于 $1 \bmod 4$, 则 $p \bmod q$, $q \bmod p$ 的情况是一样的; 如果 p 和 q 都是同余于 $3 \bmod 4$, 则它们的情况相反. 但是勒让德的证明是有毛病的. 到 1796 年左右, 高斯得到了第一个严格的证明 (而且他最终一共得到了 8 个不同的证明). 在 19 世纪 20 年代, 高斯就双二次等价性提出了类似问题, 即 $x^4 \equiv p \bmod q$ 与 $y^4 \equiv q \bmod p$ 相互关系的问题. 正是由于企图回答这个新问题, 使得高斯提出了高斯整数, 而且发出了一个信号: 更高次剩余理论需要其他类型的 "整数". 虽然艾森斯坦、狄利克雷[VI.36]、厄尔米特、库默尔[VI.40]、克罗内克[VI.48] 等人都按照高斯的精神把这些思想推向前进, 直到戴德金[VI.50] 在 1871 年为狄利克雷的《数论讲义》(*Vorlesongen Über Zahlentheorie*) 所写的第 10 个附录才基本上通过提出新概念, 不是由数论的观点, 而是由集合论的观点, 公理化地重新处理这个问题. 例如提出了一些一般概念 —— 但还不是精确的公理化的定义 —— 如域、环、理想[III.81 §2] 和模[III.81 §2], 而用这些新的抽象结构来分析他的数论背景. 从哲学角度看来, 他的战略和伽罗瓦的并无大异: 把手头的 "具体" 问题, 翻译为新的更加抽象的语言, 使得能在 "更高" 的层次上更干净地加以解决. 到了 20 世纪初, 艾米 · 诺特[VI.76] 和她的学生们, 其中就有范德瓦尔登 (Bartel Leendert van der Waerden, 1903–1996, 荷兰数学家), 把戴德金的思想推向前进, 有助于创造一种从结构的角度看待代数的途径, 这对于 20 世纪的数学是一个特征.

与欧洲大陆上 19 世纪 "数" 的概念的数论性质的演化相平行, 产生了一组非常不同的发展方向, 首先发生在英伦诸岛. 从 18 世纪晚期, 英国的数学家们就不仅就数的性质在辩论 —— 例如辩论 "负数和虚数有意义吗" 这样一些问题 —— 还就代数的意义也在辩论 —— 例如 "在 $ax + by$ 这样的表达式中, a, b, x 和 y 取哪些值是合法的, 而 '+' 又意味着什么" 这样的问题. 在 19 世纪 30 年代, 爱尔兰数学家哈密顿[VI.37] 提出了对于复数的 "统一的" 解释, 而原来的情况在他看来是回避了一个逻辑问题: 实数加虚数, 犹如桔子加苹果, 是什么意思? 给定了实数 a 和 b 以后, 哈密顿把复数 $a + b\sqrt{-1}$ 想作是一个有序对 (哈密顿称之为一个 "偶")(a, b). 然后, 他就来定义这些偶的加、减、乘、除. 当他认识到这也提供了一个表示复平面上的点的方法以后, 他自然地就会问, 能否构造一种代数的有序三元组来表示 3 维空间的点. 在对这个问题作了 10 年时断时续的沉思以后, 哈密顿最终不是用三

元组, 而是用四元组回答了这个问题, 这就是所谓*四元数*[III.76]. 四元数就是这样的 "数": $(a,b,c,d)=a+b\mathrm{i}+c\mathrm{j}+d\mathrm{k}$, 其中 a,b,c 和 d 是实数, 而 $\mathrm{i},\mathrm{j},\mathrm{k}$ 满足以下的关系式: $\mathrm{ij}=-\mathrm{ji}=\mathrm{k},\mathrm{jk}=-\mathrm{kj}=\mathrm{i},\mathrm{ki}=-\mathrm{ik}=\mathrm{j};\mathrm{i}^2=\mathrm{j}^2=\mathrm{k}^2=-1$. 和在 2 维情况一样, 加法可以按分量来定义, 而乘法则是这样定义的: 虽然每一个非零元都有乘法逆, 但是却是不可交换的. 这样, 新的数系不服从算术的 "通常的" 法则.

虽然, 英国的哈密顿的同时代人中, 有一些人质问: 数学家有多大的自由来创造新的数学世界, 另一些人如凯莱立刻把这个思想向前发展, 提出一种八元数, 其乘法不仅是不可交换的, 后来还发现甚至不适合结合律. 对于这种系统自然发生了一些问题, 但是哈密顿本人就提出了以下的问题, 即如果系数域, 或称基域, 不是实数而是复数, 又会发生什么情况? 这时, 容易看到两个复四元数 $(-\sqrt{-1},0,1,0)=-\sqrt{-1}+\mathrm{j},(\sqrt{-1},0,1,0)=\sqrt{-1}+\mathrm{j}$ 的乘积是 $1+\mathrm{j}^2=1+(-1)=0$. 换句话说, 复四元数中有零因子, 即相乘以后得零的非零元素 —— 这是另一个把它们与整数的性质基本区别开来的性质. 在下面这些数学家们的努力下, 这一条思路导致了一种能够自立的数学结构的出现, 这种结构叫做 "代数"[1], 这些数学家中有皮尔斯 (Benjamin Peirce, 1809–1880, 美国数学家)、*弗罗贝尼乌斯*[VI.58]、George Scheffers (1866–1945)、Theodor Molien(1866–1945, 德国数学家)、*嘉当*[VI.69]、Joseph H. M. Wedderburn (1882–1948, 美国数学家) 等. 这个发展自然地和矩阵理论 ($n\times n$ 矩阵在其基域上构成一个 n^2 维的代数) 通过高斯、凯莱和西尔维斯特的工作结合起来. 它也和并非无关的向量空间融合起来 (n 维代数就是除加法和内积以外还有一个向量乘法的 n 维向量空间), 这是来自类似于格拉斯曼 (Hermann Gunther Grassmann, 1809–1877, 德国数学家) 的某些思想的.

9. 现代代数

到了 1900 年, 许多代数结构已经被确认了, 其性质也被探讨了. 原来各在自己的背景下的孤立的结构现在也在其他背景下被发现了, 有时还全是意料之外的事. 这样, 这些结构比起原来发现它们时人们所了解的在数学上还要更加一般. 在 20 世纪的前几十年里面, 代数学家 (这个名词当时还不算是非历史的) 越来越认识到这些共同点 —— 即它们都具有群、环、域这些结构 —— 而在更抽象的水平上考虑问题. 例如有哪些有限单群? 它们能否分类 (见*有限单群的分类*[V.7])? 此外受到*康托*[VI.54]、希尔伯特和其他人的集合论和公理化的工作的启示, 他们也欣赏起分析的公共标准, 并且把公理化给分析带来的 [结果与自己领域的情况] 加以比较. 例

①"代数" 一词现在有了两种意义: 一是作为一个数学分支, 即本文的主题; 二是作为一种代数结构, 其地位如同前面讲过的群、环、域一样, 是由一组公理来定义的. 这里没有详细讲这些公理是什么 —— 当然也没有详细讲群、环、域的公理定义. 在本文前面两次提到 "代数理论"(见下文), 那里的 "代数" 都是第二种意义下的. —— 中译本注

如斯坦尼兹 (Ernst Steinitz, 1871–1928, 德国数学家) 在 1910 年给出了域的抽象理论的基础工作, 而四年以后, 弗朗克尔 (Adolf Abraham Halevi Fraenkel, 1891–1965, 德国数学家) 也对环的理论做了这件事. 当范德瓦尔登在 19 世纪 20 年代末认识到这些可以解释为: 在基本原则上与希尔伯特在不变式理论中的工作、与戴德金和艾米 · 诺特在代数数论中的工作都互相吻合. 这样一种解释在 1930 年就成了范德瓦尔登的经典的教科书《近世代数》(*Moderne Algebra*)[①], 成了以结构为指向的 "现代的代数学" 的典范, 而包含了中学教的多项式代数, 而且仍然刻画了今天的代数思想.

进一步阅读的文献

Bashmakova L, and Smirnova G. 2000. *The Beginnings and Evolution of Algebra.* translated by Shenitzer A. Washington, DC: The Mathematival Association of America.

Corry L. 1996. *Modern Algebra and the Rise of Mathematical Structures.* Science Network, volume 17. Basel: Birkhäuser.

Edwards H M. 1984. *Galois Theory.* New York: Springer.

Heath T L. 1956. *The Thirteen Books of Euclid's Elements*, 2nd edn. (3 vols.). New York: Dover.

Høyrup J. 2002. *Lengths, Widths, Surfaces: A Portrait of Old Babylonian Algebra and its Kin.* New York: Springer.

Klein J. 1968. *Greek Mathematical Thought and the Origin of Algebra.* Translated by Braun E. Cambridge, MA:The MIT Press.

Netz R. 2004. *The Transformation of Mathematics in the Early Mediterranean World: From Problems to Equations.* Cambridge: Cambridge University Press.

Parshall K H. 1988. The art of algebra from al-Khwārizmī to Viète. A study in the natural selection of ideas. *History of Science*, 26: 129-64.

—. 1989. Towards a history of nineteenth-century invariant theory // *The History of Modern Mathematics.* Edited by Rowe D E and McCleary J, volume I, 157-206. Amsterdam: Academic Press.

Sesiano J. 1999. *Une Introduction à l'Histoire de l'algèbre: Résolution des équations des Mésopotamiens à la Renaisance.* Lausane: Presses Polytechnique et Universitaires Romandes.

Van der Waerden B. 1985. *A Hietory of Algebra from al-Khuārizm ī to Emmy Noether.* New York: Springer.

Wussing H. 1984. *The Genisis of the Abstract Group Concept: A Contribution to the*

①此书在 1960 年第二版就改名为《代数学》, 中译本和英译本都是如此. 对此, 范德瓦尔登解释说, 在 1930 年还可以称为是现代的代数学 (我国文献有时用近世代数学的说法), 在今天, 这就是代数学了. —— 中译本注

History of the Origin of Abstract Group Theory. Tanslated by Shenitzer A. Cambridge MA: The MIT Press.

II.4 算 法

Jean-Luc Chabert

1. 什么是算法

对于 "算法" 一词给以精确的定义不是一件容易事, 有一些意义相近的同义语, 就是一些其他的名词, 它们 (有时) 会给出差不多同样的东西, 例如 "法则""技巧""程序" 还有 "方法" 等等都是这种同义语. 也可以给出一些例子, 如长乘法, 就是小学生学的把两个正整数相乘的竖式乘法. 然而, 虽然非形式的解释和选得很恰当的例子对于什么是算法给出了很好的感觉, 但算法一词中所深藏的思想却经历了一个很长的演化历程, 直得到 20 世纪才得到了令人满意的形式定义, 而关于算法的观念, 直到如今还在演进. 本文中, 我们试图对这个发展作一些解释, 来弄清在当代这个名词的意义.

1.1 算盘家和算法家

回到关于乘法的例子, 有一点是显然的: 怎样把两个数相乘? 表示这些数的方法极大地影响了乘法的具体作法. 为了弄明白这点, 请试着把两个罗马数字 CXLVII 和 XXIX 相乘, 但不要先把它们译成等价的十进数字 147 和 29. 这件事既难弄明白, 明白了以后进行计算也极其花时间, 而这就可以解释何以留存至今的罗马帝国关于乘法的材料极为零散. 记数制度可以是 "累加的", 如罗马记数法: [C 表示 100, X 表示 10, L 表示 50, 但是 X 放在 L 左方表示要从 L 中减去 X, 所以就是 40, V 表示 5, I 表示 1, 两个 I 放在 V 的右方, 表示要把它们加到 V 上, 所以是 7. 把所有以上的解释 "累加" 起来, 就是罗马数学的 147]. 记数制度也可以是**进位的**, 如我们今天所用的那样. 如果是进位的, 可以使用一个或多个基底 —— 例如苏末人[①]就既使用 10, 又使用 60 为基底.

在很长的时期中, 进行计算可以使用一种计算工具 "abacus". [这个字通常译为算盘, 因为中国使用的算盘也属于这一类, 其实它的历史源流很长, 包括了许多不同民族使用的计算工具], 最初它就是在沙地上画出的线条, 然后把小石子放在这些线条上进行计算. [实际上, abacus 字源是拉丁文, 意为沙盘]. (同样, 计算这个词, 来自拉丁文的 calculus, 原意就是小石子). 后来就有了计算版, [它是一些民族使用的计算工具, 是在木板上刻了横的或竖的沟槽], 把标记物 (例如小石子) 放在槽里

①就是从数到数系[II.1] 里讲到的美索不达米亚的古老民族. —— 中译本注

作计算. 这些计算工具可以表示一定基底下的进位制的数. 例如, 如果以 10 为基底, 则一个标记物可以代表 1 个单位, 或者 10, 或者 100 等等, 视它是放在哪一横行或竖列而定. 按照精确的规则移动这些标记物, 就可以进行算术四则运算. 中国的算盘就是 abacus 的一种.

到 12 世纪, 阿拉伯数学著作被翻译为拉丁文以后, 十进制就在欧洲流行开来了. 这种进位制特别适合于算术运算, 并且引导到许多新的计算方法. 这些方法就通称为**算法**(algoritmus), 而与在算盘上用标记物进行计算相区别.

虽然数字符号, 就是数码, 来自印度人的实践, 而后来才为阿拉伯人所知, 现在这些数码却叫做阿拉伯数码. 算法 (algorithm) 的字源却是阿拉伯文, 它是阿拉伯数学家阿尔 · 花拉子米[VI.5] 的名字的变体. 阿尔 · 花拉子米是现在已知的最古老的数学书的作者, 这一著作名为 *al-Kitāb al-mukhtasar fi hisāb al-jabr wa'l-muqābala* (《通过补全和还原作计算的纲要》), 其中的 *al-jabr* 后来就变成了 "代数"(algebra) 一词.

1.2 有限性

我们已经看到 "算法" 一词在中世纪是指以整数的十进制表示为基础的计算程序. 但是到了 17 世纪, 在达朗贝尔[VI.20] 主编的《百科全书》(*Encyclopédie*) 中, 算法一词被赋予了更广泛的意义, 不只用于算术, 还用于关于代数方法以及其他的计算程序, 诸如 "积分学的算法" "正弦的算法" 等等.

算法这个词又逐渐地被用来表示任意的具有精确规则的系统的计算程序. 最后, 随着计算机的作用越来越大, **有限性**的重要性被充分认识到了, 很本质的要求是, 这个过程在有限时间以后就会停止, 而给出结果. 所以就得到了下面的朴素的定义:

一个算法就是有限多个规则的集合, 用以对数量有限的数据进行操作, 而在有限多步以后产生结果.

注意, 在这里一直强调有限性, 在写出算法时的有限性, 以及在执行算法时的有限性.

上面的陈述当然算不上是在定义一词的经典意义下的数学定义. 我们将会看到, 把它进一步形式化是重要的. 但是我们现在暂时也就满足于这个 "定义" 了, 而且来看一下数学中的算法的一些经典例子.

2. 三个历史上的例子

算法具有一种我们尚未提到的特性: **迭代**, 也就是简单程序的反复执行. 为了看清迭代的重要性, 我们再一次来看一下长乘法这个例子, 这是一个对任意大小的正整数都适用的方法. 数字变得越大, 程序也就越长. 但是最关紧要的是, 方法是

"同样的", 如果会把两个三位数相乘, 也就会把两个 137 位的数字相乘, 而不必再去学什么新的原理 (哪怕感到厌烦而不想去算了). 理由在于长乘法的方法里面包含了大量的仔细构造好的小得多的任务的重复执行, 例如把两个一位数相乘的九九表. 我们将会看到, 迭代在本节所要讨论的算法中都起了重要作用.

2.1 欧几里得算法: 迭代

欧几里得算法[III.22]是说明算法本质的最好也是最常用的例子. 这个算法可以追溯到公元前 3 世纪. 欧几里得[VI.2] 用它来计算两个正整数的**最大公约数**(gcd)(有时也称为**最高公因子**(hcf).

当我们最开始遇到两个正整数 a 和 b 的最大公约数时, 它是定义为一个正整数, 而且同为 a 和 b 的因数 (或因子). 然而, 为了很多目的, 定义它为具有以下两个性质的唯一的整数 d 更好. 这两个性质就是: 首先, d 是 a 和 b 的一个因数; 其次, 如果 c 是 a 和 b 的另一个因数, 则 d 可以被 c 所整除. 欧几里得的《几何原本》卷Ⅶ的前两个命题给出了求 d 的方法, 其中第一个命题如下: "给定了两个不相等的数, 从较大的一数不断地减去较小的一数, 如果余下的数位, 都不能量度前数, 直到余下的数为一单位为止, 这时, 原来的数为互质." 换句话说, 如果辗转相减得到了数 1, 则 gcd 为 1. 这时, 就说原来的两个数**互质**(或**互为素数**).

2.1.1 辗转相减法

现在我们来一般地描述欧几里得算法, 它是基于以下两点观察的:

(i) 如果 $a = b$, 则 a 和 b 的 gcd 就是 b(或 a).

(ii) d 是 a 和 b 的公约数, 当且仅当它也是 $a - b$ 和 b 的公约数.

现在设要求 a 和 b 的 gcd, 而且设 $a \geqslant b$. 如果 $a = b$, 则观察 (i) 告诉我们, gcd 就是 b. 若不然, 观察 (ii) 告诉我们, 如果求 $a - b$ 和 b 的 gcd 也会得到同样的答案. 现在令 a_1 是 $a - b$ 和 b 中较大的一个, 而 b_1 则为其中较小的一个 (当然, 如果它们相等, 则令 $a_1 = b_1 = b$), 然后再来完成开始时所给的任务 —— 求两数的 gcd—— 不过, 现在两数中较大的一个, 即 a_1, 小于原来两数中较大的一个, 即 a. 这样我们就可以把上面的程序再重复一遍: 若 $a_1 = b_1$, 则 a_1 和 b_1 的 gcd, 亦即 a 和 b 的 gcd 是 b_1, 若不然, 就把 a_1 换成 $a_1 - b_1$, 再来组织 $a_1 - b_1$ 和 b_1, 总之, 较大的一个要放在前面, [然后再继续下去, 这就叫做 "辗转相减"].

为了使这个程序能够进行下去, 还有一个观察是需要的, 这就是下面的关于正整数的一个基本事实, 有时称为良序原理:

(iii) 严格下降的正整数序列 $a_0 > a_1 > a_2 > \cdots$ 必为有限序列.

因为上面的迭代程序恰好产生了一个严格下降序列, 这个迭代最终一定会停止, 这就意味着在某一点上必有 $a_k = b_k$, 而这个公共值就是 a 和 b 的 gcd(见图 1).

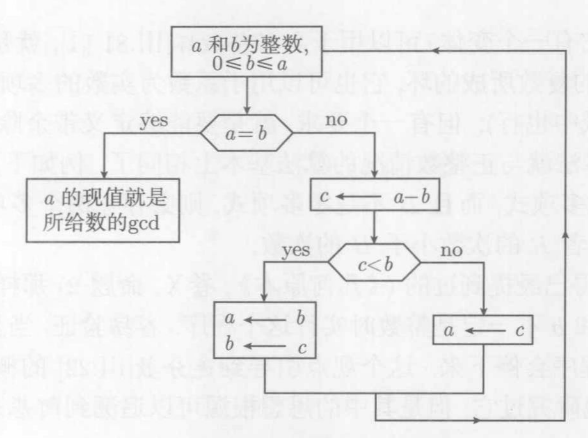


图 1 欧几里得算法的流程图

2.1.2 欧几里得除法

通常对于欧几里得算法的陈述与此稍有不同. 可以应用一种较复杂的程序, 称为**欧几里得除法**—— 也就是带余除法 —— 它可以大大减少算法的步数, [所以这种算法也称为**辗转相除法**]. 这个程序的基本事实是: 若 a 和 b 是两个正整数, 则必存在唯一的整数 q 和 r, 使得

$$a = bq + r, \quad 0 \leqslant r < b.$$

数 q 称为**商**, 而 r 称为**余数**. 上面的两点说明 (i) 和 (ii) 现在要代以

(i)′ 若 $r = 0$, 则 a 和 b 的 gcd 就是 b.

(ii)′ a 和 b 的 gcd 与 b 和 r 的 gcd 是相同的.

这一次, 在第一步要用 (b, r) 代替 (a, b). 如果 $r \neq 0$, 则还要做第二步, 并用 (r, r_1) 来代替 (b, r), r_1 是用 r 去除 b 所得的余数, [所以 $r_1 < r$], 并仿此以往. 这样, 就得到余数的序列是严格下降的 $(b > r > r_1 > r_2 \geqslant 0)$. [再用一次良序原理], 即知这个程序经过有限步后一定停止, 而最后一个非零的余数就是 a 和 b 的 gcd.

不难看到, 这两种方法, [就求 gcd 而言] 是等价的, [但就算法而言则有很大区别]. 例如, 设 $a = 103\,438, b = 37$. 如果用辗转相减法, 就要从 103 438 中累次减去 37, 一直到余下的差数小于 37 为止. 这个差数与 103 438 除以 37 的余数是一样的, 而如果用第二种方法, 一次就可以得到它. 这样, 使用第二种方法的理由就在于用累次减法来求除法的余数是非常低效率的. 效率上的收益在实践上是很重要的, 第二种方法给出的是多项式时间算法[IV.20 §2], 而第一种方法所需的则是指数长的时间.

2.1.3 推广

欧几里得算法可以推广到许多其他背景下, 只要在那里有加法、减法和乘法的

概念就行. 例如它有一个变体, 可以用于高斯整数环[III.81 §1], 就是形如 $a+bi$, 而其中 a, b 为整数的复数所成的环, 它也可以用于系数为实数的多项式环中 (就此而论, 系数在任意域中也行). 但有一个要求, 就是要能够定义带余除法的类比物, 有了这一点以后, 算法就与正整数情况的算法基本上相同了. 例如下面的命题: 设 A 和 B 是两个任意多项式, 而且 B 不是零多项式, 则必存在两个多项式 Q 和 R, 使得或者 $R=0$, 或者 R 的次数小于 B 的次数.

正如欧几里得已经提到过的 (《几何原本》, 卷 X, 命题 2) 那样, 也可以对于一对数 (a, b) 当 a 和 b 不一定是整数时实行这个程序. 容易验证, 当且仅当比 a/b 是有理数时, 这个程序会停下来. 这个观点引导到连分数[III.22] 的概念. 在 17 世纪以前, 没有特别地研究过它, 但是其中的思想根源可以追溯到阿基米德[VI.3].

2.2　阿基米德计算 π 的方法: 逼近和有限性

圆周长和圆的直径的比值是一个常数, 而自从 18 世纪以来就记作 π(参看 [III.70]). 现在我们来看一看阿基米德怎样在公元前 3 世纪就得到了这个比值的经典的近似值 22/7. 若在圆内作一个内接的正多边形 (其顶点都在圆周上), 又作其外切的正多边形 (其边都是圆周的切线), 再计算这些多边形的周长, 就会得到 π 的下界与上界, 因为圆的周长必定大于任意内接多边形的周长, 而小于任意外切多边形的周长 (见图 2). 阿基米德从正六边形开始, 然后, 每次把多边形的边数加倍, 得到了越来越精确的上下界. 他做到九十六边形为止, 得到了

$$3+\frac{10}{71} \leqslant \pi \leqslant 3+\frac{1}{7}.$$

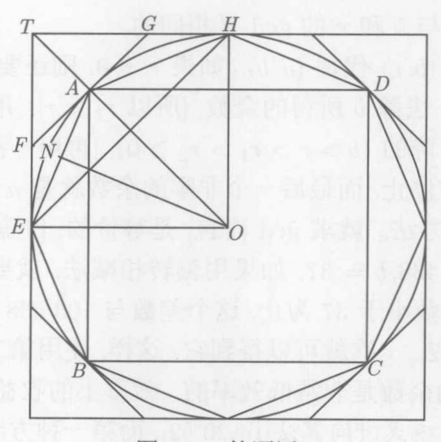


图 2　π 的逼近

这个过程中显然涉及迭代. 但是称它为一个算法对不对? 严格地说, 它不是一个算法, 不论取多少边的多边形, 所得到的仅是 π 的近似值, 所以这个过程不是有

限的. 然而我们确实得到了一个可以近似计算 π 到任意精确度的算法. 例如, 如果想得到 π 的一个准确到小数十位的近似值, 经过有限多步以后, 这个算法会给出一个. 重要的是, 这个过程是**收敛的**. 就是说, 重要的在于由迭代得出之值可以任意地接近于 π. 这个方法的几何来源可以用来证明这个收敛性, 而 1609 年德国人 Ludolph van Ceulen [基本上用阿基米德的方法] 作到了 2^{62} 边形, 得到 π 的精确到小数 35 位的近似值①.

然而, 逼近 π 的算法与阿基米德计算两个正整数的 gcd 的算法有一个清楚的区别. 如欧几里得那样的算法时常称为离散算法, 而与用来计算非整数值的数值算法相对立 (见数值分析[IV.21]).

2.3 牛顿–拉夫森方法: 递推公式

1670 年前后, 牛顿[VI.14] 提出了一个求方程之根的方法, 而且就方程 $x^3-2x-5=0$ 解释了他的方法. 他的解释从下面的一个观察开始: 根 x 近似地等于 2. 于是他写出 $x=2+p$, 并用 $2+p$ 代替原方程的 x, 而得到了一个关于 p 的方程. 这个新方程算出来是 $p^3+6p^2+10p-1=0$. 因为 x 接近于 2, 所以 p 很小, 而他就略去了 p^3 和 $6p^2$(它们比 $10p-1$ 是相当的小) 来估计 p. 这就给了他 p 的方程 $10p-1=0$, 即 $p=1/10$. 这当然不是一个准确解, 但是, 给了牛顿关于根的新的更好的近似值: $x=2.1$. 然后牛顿就重复这个过程, 令 $x=2.1+q$, 代入原方程以后又给出了一个关于 q 的方程, 近似地解这个方程, 又把他的近似解精确化了, 于是得到 q 的估计为 -0.0054, 所以 x 的下一个近似值是 2.0946.

尽管如此, 我们怎么能确定这个过程会收敛于 x 呢? 让我们更仔细地考察这个方法.

2.3.1 切线和收敛性

牛顿的方法可以从几何上用函数 f 的图像来解释, 虽然牛顿本人并没有这样做. $f(x)=0$ 的每一个根 x 都对应于函数 $y=f(x)$ 的曲线和 x 轴的一个交点. 如果从根 x 的一个近似值 a 开始, 而且和上面做的一样, 设 $p=x-a$, 于是可以用 $a+p$ 代替 x 而得到一个新的函数 $g(p)$, 也就是说把原点 $(0,0)$ 有效地移到了 $(a,0)$ 处. 然后把 p 的所有高次幂都略去, 只留下常数项和线性项, 这样就得到了函数 g 的最佳的线性逼近 —— 从几何上说, 这就是 g 在点 $(0,g(0))$ 处的切线. 这样, 对于 p 所得到的近似值就是函数 y 在点 $(0,g(0))$ 处的切线与 x 轴的交点. 再在横坐标上加一个 a, 也就是让原点回到原来的 $(0,0)$ 处, 这样 $a+p$ 就给出了 f 的根的新近似值. 这就是牛顿的方法称为**切线法**的原因 (图 3). [从图 3 上可以看到, 再作一

①Ludolph van Ceulen 和那个时代许多德国人一样, 因为畏惧宗教裁判所的迫害, 逃到了荷兰, 终生居于雷顿城. 他得到的 π 的近似值是 3.14159265358979323846264338327950288, 后来被人称为 Ludolph 数. —— 中译本注

次切线的逼近, 如果曲线 $y=f(x)$ 与 x 轴的交点在 a 点以及 f 在点 $(a,f(a))$ 处的切线与 x 轴的交点 (即图 3 上的横坐标为 $a+p$ 的点, 即根的近似值) 之间, 则第二次的近似值 (即图 3 上的 $a+p+q$) 肯定比第一次的近似值 $a+p$ 好[①] (这里称 a 为根的零次近似)].

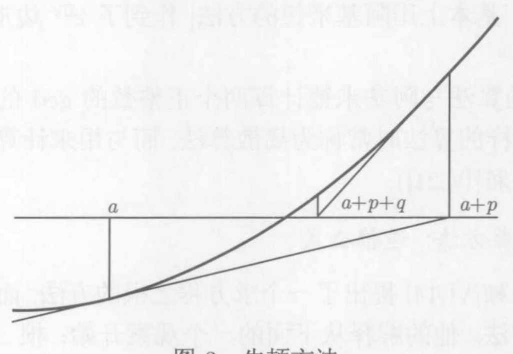


图 3　牛顿方法

回到牛顿的例子, 可以看到牛顿选取 $a=2$ 并不是上面所说的情况. 但是从下一个近似值 2.1 开始, 以下所有的近似值就都是这个情况了. 从几何上看, 如果点 $(a,f(a))$ 位于 x 轴的上方, 而且 $y=f(x)$ 的曲线在凸部与 x 轴相交, 或者点 $(a,f(a))$ 在 x 轴的下方, 而且 $y=f(x)$ 曲线在凹部与 x 轴相交 (即图 3 上的情况), 就会出现这种有利的情况. 在这些情况下, 只要根不是重根, 这里的收敛性是**平方的**, 即每一步的误差都是上一步的误差的平方数量级 —— 换一个等价的说法, 就是每一往下走一步, 有效的小数位数都会加倍. 这就是极快的了.

初始的逼近 (即零次近似) 的选择显然是很重要的, 而且提出了微妙的未曾想到的问题. 如果我们考虑复多项式的复根, 这就更加清楚了. 牛顿的方法很容易适应这个更广泛的背景. 设 z 是一个复多项式的复根, 而 z_0 是初始的逼近, 于是牛顿方法将给出一个序列 $z_0,z_1,z_2,\cdots$, 它可能收敛于 z, 也可能不收敛. 我们定义根 z 的**吸引区域**为这样的初始逼近 z_0 的集合, 使得所得到的序列确实收敛于 z, 并且记这个区域为 $A(z)$. 怎样来决定 $A(z)$ 呢?

第一个问这个问题的人是凯莱[VI.46], 时间是 1879 年. 他注意到, 对于二次多项式, 这个问题是很容易的, 但当次数为 3 或者更大时, 问题就很困难了. 例如多项式 z^2-1 的根 ± 1 的吸引区域分别是复平面上以铅直轴为界的两个半平面, 但是 z^3-1 的三个根 $1,\omega,\omega^2$ 的相应的吸引区域就是极复杂的集合. 这些集合是由儒利亚 (Gaston Maurice Julia, 1863–1978, 法国数学家) 在 1918 年描述的, 而现在称为分形集合. 牛顿方法和分形几何都将在条目*动力学*[IV.14] 中更详细地研究.

①这一段中文译文与原文略有不同. —— 中译本注

2.3.2 递推公式

牛顿方法的每一阶段都会产生一个新方程. [原来是 x 的方程, 在引入新的变量 p 以后得到 p 的方程 $g(p)=0$, 再以后又有 q 的方程, 而每一个新方程又都要用切线方法求其近似解]. 但是拉夫森 (Joseph Raphson, 1648–1715, 英国数学家) 指出实际上并无必要. 他就特殊的例子给出在每一步都可以使用的单一一个公式. 但是他的基本的观察可以一般地适用, 导出可以用于每一个情况的一般公式, 而这个公式用切线的解释就可以容易得出. 事实上, 曲线 $y=f(x)$ 在 x 坐标为 a 处的切线方程是 $y-f(a)=f'(a)(x-a)$, 它与 x 轴的交点的横坐标是 $a-f(a)/f'(a)$, [就是图 3 上的 $a+p$]. 我们现在所说的牛顿–拉夫森方法就是指的这个公式. 我们从一个初始逼近 $a_0=a$ 开始再用这个递推公式得出

$$a_{n+1}=a_n-\frac{f(a_n)}{f'(a_n)},$$

[这样就得到一个逼近的序列, 在复情况下, 也就是前面说的 $z_0,z_1,z_2,\cdots$].

作为一个例子, 考虑函数 $f(x)=x^2-c$. 这时, 牛顿方法就给出 c 的平方根 $\sqrt{c}$ 的一串近似值, 递推公式现在成了$a_{n+1}=\frac{1}{2}(a_n+c/a_n)$(在上面的一般公式中把 f 换成 x^2-c 即得). 这个近似平方根的求法, 公元 1 世纪的亚历山大里亚的海伦就已经知道. 注意, 如果 a_0 接近于$\sqrt{c}$, c/a_0 也接近于 $\sqrt{c}$, 实际上 $\sqrt{c}$ 在二者之间, 而且是二者的算术平均: $a_1=\frac{1}{2}(a_0+c/a_0)$.

3. 是否总有算法存在

3.1 希尔伯特第十问题: 形式化的必要性

在 1900 年的第二届国际数学家大会上, 希尔伯特[VI.63] 提出了 23 个问题. 这些问题以及希尔伯特的一般的工作在 20 世纪对于数学有巨大的影响 (Gray, 2000). 我们这里感兴趣的是**希尔伯特第十问题**: 给定一个丢番图方程, 就是一个有任意多个未定元的整数系数的多项式方程, “要求找出一个程序, 按照它, 可以经过有限多次运算, 来决定此方程是否在整数中有解”. 换言之, 我们需要找到一个算法, 使得任给一个丢番图方程, 它都能告诉我们此方程是否至少存在一个整数解. 当然, 对于许多丢番图方程, 很容易找到一个解, 或者证明它没有解存在. 然而情况并不总是这样, 费马方程 $x^n+y^n=z^n\ (n\geqslant 3)$ 就是一个例子 (甚至在费马大定理[V.10] 得到证明以前, 对任意特定的 n 就已经有算法存在, 能够决定此方程是否有解存在. 但是, 我们不能说这是容易的).

如果对于一个丢番图方程, 希尔伯特的问题的答案是正面的, 我们就可以拿出一个希尔伯特所要求的那一类 “程序” 来证明它. 为此倒不必对于什么叫做 “程序” 有一个准确的理解. 然而, 如果想给出**否定的**答案, 那么就得证明**没有算法存在**, 为

此就必须说明白什么才算是一个算法. 在 §1.2 中我们曾经给出了算法的一个定义, 看来已经足够精确了, 但是, 要考虑希尔伯特第十问题, 这个定义就还不够精确. 在那里, 我们曾经谈到过 "规则", 但是在算法里究竟允许哪一类规则呢? 我们怎么能够确定, 完成某个任务, 究竟是没有算法存在, 还是我们找不出来呢?

3.2 递归函数: 丘奇的论题

我们需要的就是算法这个概念的形式定义. 早在 17 世纪, 莱布尼兹[VI.15] 就已经设想有一种万有的语言, 使我们能够把数学证明归结为简单的计算. 到了 19 世纪, 一批逻辑学家如巴贝奇 (Charles Babbage, 1791–1871, 英国人, 现代计算机的先驱者之一)、布尔[VI.43]、弗雷格[VI.56]、佩亚诺[VI.62] 都试图通过逻辑的 "代数化" 来把数学推理形式化. 最后, 到了 1931 年至 1936 年之间, 哥德尔[VI.92]、丘奇[VI.89] 和克林 (Stephen Cole Kleene, 1909–1994, 美国数学家) 引入了**递归函数**的概念 (见 (Davies, 1965), 这是一本论文集, 收录了上述诸文). 粗略地说, 一个递归函数就是可以通过算法的手段来计算的函数. [虽然它的基本思想可以这样粗略地表示], 但是递归函数的**定义**却不同, 它是完全精确的.

3.2.1 原始递归函数

递归函数的另一个粗略的定义如下: 一个递归函数就是一个可以归纳地定义的函数. 为了说明这是什么意思, 让我们把加法和乘法考虑为由 $N \times N$ 到 N 的函数. 为了强调这一点, 把 $x+y$ 和 xy 分别记成 $\mathrm{sum}(x,y)$ 和 $\mathrm{prod}(x,y)$.

关于乘法, 有一个我们熟悉的事实: 乘法就是 "累加". 现在我们更精确地考察这个思想. 我们可以通过下面两条规则来用函数 "sum" 定义函数 "prod". 规则之一是 $\mathrm{prod}(1,y)=y$; 其二是 $\mathrm{prod}(x+1,y)=\mathrm{sum}(\mathrm{prod}(x,y),y)$. 这样, 如果知道了如何计算 $\mathrm{prod}(x,y)$, 又知道了如何计算函数 sum, 就会计算 $\mathrm{prod}(x+1,y)$. 因为又知道了如何计算 "基础情况" $\mathrm{prod}(1,y)$, 它就是 y 本身, 再作简单的归纳论证就完全决定了函数 "prod".

我们刚才见到的就是一个函数如何用另一个函数来 "递归地定义". 现在想要了解所有由 N^n 到 N 的可以用少数几个方法建造起来的函数之类, 而递归只是这少数几个方法之一. 把由 N^n 到 N 的函数称为 ***n*元函数**.

一开始, 需要有函数的一个初始的储备, 其余函数都要从这个初始储备建造出来. 事实表明, 函数的一个非常简单的集合就已经足够了. 最基本的是**常值函数**, 就是把 N^n 中的任意 n 元组都变为一个固定正整数 c 的函数. 另一个很简单的函数是**后继元函数**, 它把任意正整数 n 变为它的后继元 $n+1$. 这个函数已经可以生成有趣得多的函数了. 最后还有**投影函数** U_k^n, 它把 N^n 中的 $(x_1,\cdots,x_n)$ 对应为自己的第 k 个坐标 x_k.

然后就有两个从一个函数构造出其他函数的方法. 第一个方法是**代入**, 其意义

如下：设已经有了一个 m 元函数 ϕ 和 m 个 n 元函数 $\psi_1,\cdots,\psi_m$，就可以定义一个新的 n 元函数如下：

$$(x_1,\cdots,x_n)\mapsto\phi(\psi_1(x_1,\cdots,x_n),\cdots,\psi_m(x_1,\cdots,x_n)).$$

例如 $(x+y)^2=\text{prod}(\text{sum}(x,y),\text{sum}(x,y))$，这样就从函数 "sum" 和函数 "prod" 通过代入得出了函数 $(x,y)\mapsto(x+y)^2$.

第二种构造新函数的方法是**原始递归**，它比上面用函数 "sum" 来构造函数 "prod" 的归纳方法要更一般一点. 设有一个 $(n-1)$ 元函数 ψ 和一个 $(n+1)$ 元函数 μ，这样来定义一个 n 元函数 ϕ：

$$\phi(1,x_2,\cdots,x_n)=\psi(x_2,\cdots,x_n),$$
$$\phi(k+1,x_2,\cdots,x_n)=\mu(k,\phi(k,x_2,\cdots,x_n),x_2,\cdots,x_n).$$

换句话说，ψ 告诉我们怎样得出 ϕ 的初值，即第一个坐标取 1 的值，而 μ 告诉我们怎样通过 $\phi(k,x_2,\cdots,x_n),x_2,\cdots,x_n,k$ 来得出 $\phi(k+1,x_2,\cdots,x_n)$ (上面的 sum-prod 例子更简单一些，因为其中不含有 k).

原始递归函数就是用上面的两种构造方法：代入和原始递归，从函数的初始储备所能作出的任意函数.

3.2.2 递归函数

如果想一下原始递归，而且知道一点可编程计算机的话，就会相信原始递归函数是有效的可计算的，就是说对于任何一个原始递归函数都有一个算法来计算它 (例如原始递归运算通常都可以相当直接地作为一个 FOR 循环来实现①).

逆定理是否成立？是否所有可计算函数都是原始递归的？例如考虑这样一个函数，它把正整数 n 映为 p_n 即第 n 个素数. 不难做出一个简单的算法来计算 p_n，然后这就是一个好的练习：把这个算法变成此函数为原始递归的证明 (如果想了解什么是原始递归的话).

然而，结果表明，这个函数是不典型的，有不是原始递归的可计算函数存在. 1928 年，阿克尔曼 (Wilhelm Ackermann, 1896–1962, 德国数学家) 就定义了一个函数，现在就叫做阿克尔曼函数，它有一个 "双归纳" 定义. 下面的函数和阿克尔曼函数不完全相同，但是非常相似. 这个函数 $A(x,y)$ 是由下面的递推规则决定的：

(i) 对于每一个 $y, A(1,y)=y+2$;

(ii) 对于每一个 $x, A(x,1)=2$;

(iii) 当 $x>1$ 且 $y>1$ 时，$A(x+1,y+1)=A(x,A(x+1,y))$.

例如，$A(2,y+1)=A(1,A(2,y))=A(2,y)+2$. 由此并由 $A(2,1)=2$ 这一事实可知，对于每一个 y 都有 $A(2,y)=2y$. 类似地可以证明，$A(3,y)=2^y$，而一般说来

①FOR 循环是最简单的循环子程序，它的参数有一定的有限范围，而且有一个计数器. ——中译本注

$A(x+1,y)$ 将把函数 $y \mapsto A(x,y)$"迭代". 这意味着, 即令 x 和 y 相当小, $A(x,y)$ 也可能极大. 例如, $A(4,y+1)=2^{A(4,y)}$, 所以 $A(4,y)$ 将有一个高为 y 的 "指数塔" 来表示, 有 $A(4,1)$, $A(4,2)=2^2=4, A(4,3)=2^4=16, A(4,4)=2^{16}=65536$, 而到了 $A(4,5)=2^{65\,536}$, 就大得无法在这里用十进制来表示了.

可以证明, 对于每一个原始递归函数 ϕ, 都有一个 x, 使得 $A(x,y)$ 增长得比 $\phi(y)$ 更快, 这一点可以用归纳论证来证明. 略微过分简单化一点, 如果已经证明了 $\psi(y)$ 和 $\mu(y)$ 已经增长得比 $A(x,y)$ 慢, 则由原始递归生成的函数 ϕ 也增长得更慢. 这样就可以定义一个 "对角线函数" $A(y)=A(y,y)$, 它不是一个原始递归函数, 因为它增长得比任意的 $A(x,y)$ 都更快.

如果想准确地理解哪些函数是算法地可计算的, 则我们的定义必须包括如阿克尔曼函数这样的函数, 因为它们在原则上是可计算的. 所以, 必须考虑比原始递归函数更大的函数类. 哥德尔、丘奇和克林各以不同方式做了这件事, 而得到了同样的**递归函数类**. 例如, 克林就增加了第三个他称为**极小化**的构造方法: 设 f 是一个 $(n+1)$ 元函数, 可以定义一个 n 元函数 g 如下: $g(x_1,\cdots,x_n)$ 就是满足 $f(x_1,\cdots,x_n,y)=0$ 的最小的 y(如果没有这样的 y 存在, 就说 g 对这个 $(x_1,\cdots,x_n)$ 没有定义. 但是在下文中将要略去这个复杂情况).

结果就是, 不仅阿克尔曼函数是递归函数, 而且所有可以写出一个计算机程序类似计算的函数都是递归函数. 这就给出了可计算性的形式定义, 而这是以前没有的.

3.2.3 有效可计算性

当递归函数的概念得到陈述以后, 丘奇就宣称递归函数类就是 "有效可计算" 的函数类. 这项宣布得到了广泛的相信, 但是是无法证明的. 因为递归函数概念是一个精确的数学概念, 而一个有效可计算函数只是一个直观的概念, 很像 "算法" 概念那样. 丘奇的宣布属于元数学的领域, 现在通常被称为**丘奇论题**.

3.3 图灵机

丘奇论题的最强有力的证据是: 图灵[VI.94] 在 1938 年找到了把算法概念形式化的一种看起来完全不同但图灵证明了是等价的一种表述, 那就是在他的新意义下可计算的函数都是递归函数, 其逆亦真. 他的途径是: 定义一个概念, 现在称为**图灵机**, 它可以看作一个极原始的计算机, 而在后来实际的计算机发展中起了重要的作用. 说真的, 可以在图灵机上计算的函数恰好就是在真正的计算机上可以编程计算的函数. 图灵机的原始结构, 并不使它不那么强有力, 所谓 [结构的原始性] 只是表示在它上面编程太冗长, 或硬件在执行上太麻烦. 因为递归函数就是图灵可计算函数, 所以递归函数也就是可以在真实的计算机上编程计算的函数. 所以, 不相信丘奇论题就相当于坚持有不能转变为计算机程序的 "有效程序", 而这是不可能的.

关于图灵机的描述, 可见条目计算复杂性[IV.20 §1].

图灵引入图灵机是为了回应希尔伯特第十问题的一个推广：**判定问题**(decision problem, 德文为 Entscheidungproblem). 这个问题也是希尔伯特提出的, 时间为 1922 年. 他想要知道是否存在一种 "机械的程序", 使得可以用来决定一个给定的数学命题能否证明. 图灵为了考虑这个问题, 需要对何谓 "机械的程序" 有一个精确的定义. 一旦有了图灵机这个概念以后, 他就能用一个相当直接的对角线论据证明对于希尔伯特的这个问题的答案为否. 他的论证的概要可见条目停机问题的不可解性[V.20].

4. 算法的性质

4.1 迭代对比递归

如在前面指出的, 我们时常会遇到一些计算规则, 它们在定义一个序列的元素时, 要用到序列中在它前面的元素. 这时就有两种不同的进行计算的办法. 第一个办法是**迭代**, 就是先算出第一个元素, 再用递推公式算出以下的元素. 第二个办法是**递归**, 这个办法初看起来是循环的, 因为在定义一个过程时, 用到了过程本身. 然而, 这是允许的, 因为这个过程只访问变项较小的 "本身". 递归的概念是微妙然而有力的, 让我们用一些例子来说明递归与迭代的区别.

设我们想要计算 $n! = 1\cdot 2\cdot 3\cdots(n-1)\cdot n$. 一个显然的方法是注意到这里有一个递推关系：$n! = n\cdot(n-1)!$, 还有初始值 $1! = 1$. 做完了第一步以后, 就能相继地算出 $2!, 3!, 4!$ 等等, 一直到算出 $n!$ 为止. 另一个办法是：[把计算阶乘作为一个程序, 记作 FACT], 而用 $\mathrm{FACT}(n)$ 表示执行这个程序到 $n!$ 的结果, 于是 $\mathrm{FACT}(n) = n\times\mathrm{FACT}(n-1)$, 这就是一个递归程序. 第二个办法是：为了知道如何得到 $n!$, 只需知道如何得到 $(n-1)!$, 而为了知道如何得到 $(n-1)!$, 只需知道如何得到 $(n-2)!$, 仿此类推. 因为 $1! = 1$, 所以能得到 $n!$. 这样, 递归有点像是把迭代 "倒过来" 考虑.

从某些方面来说, 用这个例子来说明这两种程序的差别是太简单了. 此外, 如果真要计算 $n!$, 则迭代比递归更加简单和自然. 现在我们再看一个例子, 这里递归就比迭代简单得多了.

4.1.1 梵天塔

梵天塔是卢卡斯 (François Édouard Lucas, 1842–1891, 法国数学家) 发明的一种数学游戏①, 设有 n 个圆盘, 大小不一, 盘的中心是一个小洞, 按大小把它们叠在

①卢卡斯主要的贡献在数论, 但是他又因 "休闲数学" 而著名. 他写过一本《数学游戏大全》, 共四卷, 是这方面的 "经典著作". 梵天塔这个游戏就出自本书第三卷. 卢卡斯在写这个游戏时, 还把它说成是来自印度教的传说, 游戏的名称 The tower of Hanoi, 其中的 Hanoi, 就是印度教的主神梵天. 在原书中, $n = 64$. 以上说明为什么把 The tower of Hanai 译为 "梵天塔". —— 中译本注

一根小柱 A 上. 大的放在下面. 还有另外两根空柱子 B 和 C. 问题是如何把原来在柱子 A 上的一摞圆盘移到柱子 B, 但要服从以下规则: 每次只许移动一个圆盘, 每一次都只能移动一根柱子最上面的圆盘放到另一根柱子上, 此外任何时刻都不许把圆盘压在较小的圆盘上, 如图 4 所示.

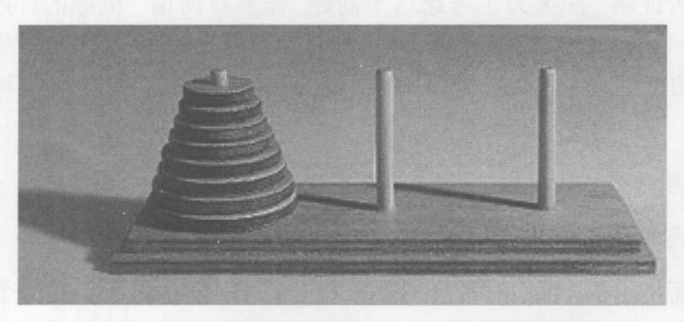


图 4　梵天塔是什么? 这里 $n=8$(中译本附图)

如果只有 3 个圆盘, 这个问题是很容易的, 但是当圆盘数目增加时, 它就急速地变得难起来了. 然而借助于递归, 就能很快地找到按照要求移动圆盘的算法了. 事实上, 假设我们已经知道移动 $n-1$ 个圆盘的程序 $H(n-1)$, 则下面就是移动 n 各圆盘的程序 $H(n)$: 先把小柱 A 上的上面 $n-1$ 个圆盘用程序 $H(n-1)$ 移到小柱 C 上, [并用 $H_{AC}(n-1)$ 记这个程序: 下标 AC 表示由小柱 A 移到小柱 C 上, 下同]; 再把 A 上的最后一个移到 B 上; 最后再用 $H(n-1)$ 把 C 上的 $n-1$ 个圆盘全部按规则移到 B 上, 而问题完全解决. 我们可以把这个递归程序用符号写为

$$H_{AB}(n)=H_{AC}(n-1)H_{AB}(1)\,H_{CB}(n-1)\,.$$

这样, $H_{AB}(n)$ 可以从 $H_{AC}(n-1)$ 和 $H_{CB}(n-1)$(它们显然都与 $H_{AB}(n-1)$ 相等) 导出. 至于 $H_{AB}(1)$ 很容易作出, 所以我们就得到了全部递归.

很容易用归纳法得出, 整个程序包含 2^n-1 步, 此外, 还能得知, 这个任务不可能以更少的步数来完成. 所以步数必为 n 的指数函数, 而对于大的 n, 这个程序是很长的.

更进一步说, n 越大, 就需要更多的存贮单元来追踪我们的程序已经进行到哪一步了. 与此相对照的是, 如果我们想在迭代程序中实行一次迭代, 我们只需要知道上一步迭代的结果就够了. 所以, 我们最需要记忆的只是一次迭代的结果. 对于梵天塔, 确实也有一个迭代程序. 描述这个程序很容易, 但是, 这个程序确实能解决问题, 却不是那么明显. 它把这 n 个圆盘的位置编码成为一个 n 位的序列, 而在每一步都给出得到下一个 n 位序列的很简单的规则. 这个规则并不参照程序已经执行了多少步, 所以, 除了用来存贮圆盘位置外, 所需记忆的量是很小的.

4.1.2 推广的欧几里得算法

欧几里得算法是很容易可以自然化为递归的另一个例子. 回忆一下, 如果 a 和 b 是两个正整数, 则可以写出 $a = qb + r,\quad 0 \leqslant r < b$. 这个算法依据的是下面的观察: gcd$(a,b)$ =gcd(b,r). 因为余数 r 很容易从 a 和 b 算出, 又因为数对 (b,r) 小于数对 (a,b), [这里大小指的是第二个分量的大小], 所以, 这就给了一个递归程序, 而在遇到 $(a,0)$ 形式的数对时就会停止.

欧几里得算法的一个重要推广是**贝祖**(Étienne Bézout, 1730-1783, 法国数学家)**引理**. 这个引理指出, 对于任意一对正整数 a 和 b, 一定存在一对整数 (不一定都为正)u 和 v, 使得

$$ua + vb = d = \gcd(a,b).$$

怎样去求这种整数 u,v 呢? **推广的欧几里得算法**给出了答案, 而它又是可以由递归来定义的. 设对于 b 和 r, 能够找到一对 (u',v') 使得 $u'b + v'r = d$ =gcd(b,r), [注意, gcd (b,r) = gcd(a,b)], 则因 $a = bq + r$, 可以把 $r = a - qb$ 代入上式, 而得 $d = u'b + v'(a - qb) = v'a + (u' - v'q)b$. 这样, 若令 $u = v', v = u' - v'q$, 就得到了 $d = ua + vb$. 因为对于 a 和 b 所需的数对 (u,v) 可以容易地从较小的 b 和 r 所需的 (u',v') 算出. 这就给了一个递归程序. $r = 0$ 就是递归的 "底", 到了那时就有 $1b + 0r = d$. 一旦到了这时, 就可以 "往回走", 通过欧几里得算法, 按照上面的规则逐步修改 (u,v). 附带请注意, 这种程序的存在, 就是贝祖引理的证明.

4.2 复杂性

迄今我们都是作为理论来讨论算法, 而忽略了它明显的实用性. 然而, 单是有算法存在, 还不一定能保证计算机能够执行它, 因为有些算法包含的步数如此之多, 使得没有一种计算机能够执行 (除非准备等上几十亿年等答案出现). 一种算法的**复杂性**, 粗略地说, 就是它完成一项任务所需的步数 (作为输入的大小的函数). 更准确地说, 这是算法的**时间复杂性**. 还有**空间复杂性**, 是指为了执行这个任务所需的存贮的多少. 复杂性理论研究的就是完成各种任务所需的计算机资源. 这个理论将在条目计算复杂性[IV.20] 中详细讨论 —— 这里只就一种算法给出检验其复杂性的一点提示.

4.2.1 欧几里得算法的复杂性

计算机执行欧几里得算法所需的时间与计算商和余数所需的时间密切相关, 也就是与递归程序访问其自身的次数密切相关. 当然, 这个数进一步又依赖于想要求其 gcd 的数 a 和 b 的大小. 一个初始的观察是: 如果 $0 < b \leqslant a$, 则 a 除以 b 的余数必小于 $a/2$. 事实上, 如果 $b > a/2$, 则 [a 除以 b 商必为 1, 而余数为 $a - b < b$; 如果 $b \leqslant a/2$, 则商为 0 而余数最多为 $b \leqslant a/2$]. 由此可知, 在求余数时, 只要计算了两步, 就可以得到一个数对, 而其第一个分量最多只有原来的第一个分量的一半,

由此容易看到, 计算余数最多只需要 $2\log_2 a+1$ 步, 而此数大体上与 a 的位数成正比, [如果采用 2 进位制, 则更清楚]. 因为一个数的位数远小于此数本身, 这个算法可以很容易地用于很大的数, 这就使它除有理论意义外, 还有很大的实用性.

所需除法的次数, 在最坏的情况下是多少, 这个问题直到 19 世纪上半叶才有人研究, 上面给出的界限 $2\log_2 a+1$ 是由芬克 (Piérre-Joseph Étienne Finck, 1797–1870, 法国数学家) 在 1841 年得出的. 但是不难看到, 这个结果可以稍加改善, 而证明当 a 和 b 是斐波那契数列的相继两项时, 算法最长. 这意味着所需除法的数目绝不会超过 $\log_\phi a+1$, 这里的 ϕ 是黄金分割.

欧几里得算法还有很低的空间复杂性. 当把数对 (a,b) 代以数对 (b,r) 后, 就可以忘掉原来的数对, 所以在任何阶段都不必记住很多东西 (也就是不必把它放在计算机的存贮内). 与此相对照, 推广的欧几里得算法表面上看, 需要记住导致 a 和 b 的 gcd$d$ 的全部计算过程, 因为这样就可以做一系列代入以得出 u 和 v 使得 $ya+bv=d$. 但是仔细看一下, 又可以看出, 在任何时刻, 只需记住少数几步, 就可以完成这个工作.

让我们用一个例子来说明这是怎么做的. 我们设 $a=38, b=21$,[很明显, $\gcd(38,21)=1$]. 现在要找出 u 和 v 使得 $38u+21v=1$. 我们从写出欧几里得算法的第一步开始:

$$38=1\times 21+17.$$

这一步告诉我们 $17=38-21$. 再作第二步:

$$21=1\times 17+4.$$

我们已经知道了如何用 38 和 21 表示 17, 把它代入上式, 就有

$$21=1\times(38-21)+4.$$

移项以后可得 $4=2\times 21-38$. 现在再来作欧几里得算法的第三步:

$$17=4\times 4+1.$$

只要记住第一步和第二步的结果, 就可以把 17 和 4 都用 38 和 21 表示, 所以再代入一次就有

$$38-21=4\times(2\times 21-38)+1.$$

整理以后就有 $1=5\times 38-9\times 21$, 而问题完全解决. [可见只需记住两步的结果].

想一想这个过程就会看到, 在每一阶段都只需要记住某两个数 [例如上面的 17 和 4] 是怎样用 a 和 b 表示的. 所以推广的欧几里得算法, 如果适当执行, 其空间复杂性也是很小的.

5. 算法的现代侧面

5.1 算法与机遇

前面曾经提到算法的概念, 甚至当它在 1920 年代和 1930 年代已经形式化了以后, 仍然在发展. 一个主要理由是认识到**随机性**对于算法可以是一个很有用的工具. 这一点初看起来可能令人迷惑, 因为算法如我们已经描绘的那样, 是决定性的程序; 我们马上就会给出一个例子, 说明随机性是怎样用上的. 第二个理由是近年来量子算法的发展, 关于这一点, 详见条目量子计算[III.74].

下面的简单例子说明机遇怎么是有用的. 给定正整数 n, 要定义一个函数 $f(n)$, 它不太难计算, 但是很难分析. 其定义如下: 如果 n 有 d 位数, 就可以逼近 $\sqrt{n}$, 使得其小数点后的前 d 个数码都是正确的 (例如应用牛顿方法), 这时就定义 $f(n)$ 等于这个第 d 位数码. 现在假设想知道, 当 n 取在 10^{30} 到 10^{31} 之间时, 使 $f(n)=0$ 的 n 占多大比例? 似乎没有一种好方法来从理论上决定这个比例; 用计算机来计算也太难, 因为在 10^{30} 和 10^{31} 之间的数又太多, 共有 9×10^{30} 个之多. 然而, 如果在 10^{30} 和 10^{31} 之间随机地取一个 10000 个数的样本, 而且就对这些数来计算使得 $f(n)=0$ 的 n 所占的比例, 这个比例将以很大的概率, 大体上等于在 10^{30} 和 10^{31} 之间使得 $f(n)=0$ 的 n 所占的比例. 所以, 如果不要求绝对的确定性, 而在概率误差很小时就满足了, 那么只需要用少得多的计算机资源就能达到目的.

5.1.1 伪随机数

然而, 怎样用一个决定性的计算机来在 10^{30} 和 10^{31} 之间选择 1 万个随机数呢? 答案是, 我们不必选随机数, 选择伪随机数几乎总是足够好了. 基本的思想可以用冯 · 诺依曼[VI.91] 在 1940 年代中期提出的方法很好的说明. 从一个 $2n$ 位正整数 a(称为 “种子”) 开始, 计算 a^2, 并从中截取出另一个新的 $2n$ 位正整数 b, 即 a^2 的第 $(n+1)$ 位到第 $3n$ 位. 然后对 b 重复以上的程序, 并仿此以往. 因为乘法会把数码都搅合起来, 所以这样得到的序列很难和真正的随机数列区别开来, 从而可以用于随机化的算法.

还有许多别的生成伪随机数序列的方法, 这就提出一个明显的问题: 一个序列应该具有哪些性质, 才能看成伪随机数序列? 这是一个复杂的问题, 对它提出过几种不同的答案. 随机算法和伪随机性, 在条目计算复杂性[IV.20 §§6, 7] 中有详细的讨论, 在那里可以找到 “伪随机生成元” 的形式定义 (还可参看条目计算数论[IV.3 §2], 其中讨论了著名的检验一个数是否素数的随机化算法). 这里讨论一个关于 0 和 1 所成的无限序列 ([以下称为 01 序列]) 的类似问题: 在什么时候能够把一个 01 序列看成是随机的?

这里又提出过许多不同的答案. 一种想法是进行简单的统计检验, 我们会期待, 0 和 1 出现的频率从长期来看应该相同, 而且更为一般的是, [我们还应该期待] 它

的任一个小的子序列, 如 00110, 也应该以 “正确的” 频率在这个待检验的 01 序列中出现 (这一个子序列出现的正确的频率应该是 1/32, 因为它的长度是 5).

然而完全可能, 一个序列可以通过这些简单的检验, 但是仍是由决定性的程序所生成的. 而且如果有一个由 0 和 1 组成的序列即令是**真正**随机的 —— 例如是由投硬币这样的方法来生成的 —— 我们还会十分怀疑, 是否还有其他决定性的算法也会生成同样这个序列. 例如, 如果一个序列是通过某种方法由 π 的数码生成的, 那么, 哪怕它通过了这些统计检验, 我们也会拒绝承认它是随机序列. 然而, 仅仅要求序列不能由递归程序生成, 还不是检验随机性的好方法. 例如取一个这样的序列而且把它的各项交替地换成 0, 就会得到一个远非随机的序列, 但是它仍然不能递归地生成.

由此原因, 冯 · 米塞斯[①]在 1919 年提出, 一个 01 序列可以称为随机的, 当且仅当不仅 0 和 1 出现的频率的极限都是 1/2, 而且, 从这个序列中 “以合理的程序提出的子序列” 也应该如此. 1940 年丘奇把 “以合理的程序提出的子序列” 翻译为 “用递归程序提出的子序列”, 从而把这一点弄明确了. 然而, 即令是这个条件仍嫌太弱: 有这样的序列, 它们并不满足所谓 “迭代对数法则”(这是一个随机序列应该满足的东西). 现在, 1966 年提出的所谓 Martin–Löf 论题是随机性最常用的定义之一: 随机序列就是能通过所有的 “有效统计序列检验” 的序列, 而这个概念我们在此不能精确地陈述了, 但是它以一种本质的方式用到了递归函数概念. 与丘奇论题相对照, 几乎所有的数学家都同意, 关于 Martin–Löf 论题还有许多讨论.

5.2　算法对于现代数学的影响

数学在自己的整个历史中都关心存在问题. 例如, 是否存在所谓*超越数*[III.41], 即不是任意整数系数的多项式的根的数? 对于这种问题, 有两类回答: 或者展示出如 π 这样的数并证明它是一个超越数 (这是林德曼 (Carl Louis Ferdinand Lindemann, 1852–1939, 德国数学家) 在 1873 年完成的); 或者给出一个 “间接的存在证明”, 如*康托*[VI.54] 证明了实数比具有整数系数的多项式的根要 “多得多”(见*可数与不可数集合*[III.11]), 由此特别可以证明, 有些实数是超越数.

5.2.1　构造主义学派

在 1910 年左右, 在*布劳威尔*[VI.75] 领导下, 数学的*直觉主义学派*[II.7 §3.1] 出现了, 这个学派拒绝排中律, 即每一个数学论断或者是真或者不真这一原理. 特别是布劳威尔不接受一个数学对象, 如超越数, 其存在性可以用反证法, 即 “若不存在将导致矛盾” 来证明. 这个学派是好几个 “构造主义” 学派的第一个, 对于这个学

①这里是指 Richard von Mises, 1883–1953, 生于乌克兰的利沃夫, 死于美国. 他在应用数学、力学、概率论和统计学方面都有贡献. 他有一个哥哥, Ludwig von Mises, 1881–1973, 则是一位著名的经济学家. —— 中译本注

派, 一个对象当且仅当它可以显示地构造出来时, 才是存在的.

做研究工作的数学家中, 赞成这些主张的人不多, 但是几乎所有的数学家都同意, 存在问题的构造性证明与间接证明有重要的差别, 而随着计算机科学的兴起, 这个差别显得更重要了. 这里面还有进一步的区分: 有时, 哪怕知道一个数学对象可以算法地构造出来, 还会关心这个算法能否在合理的短时间里构造成功.

5.2.2 有效的结果

在数论里, 有 "有效率的" 结果和 "无效率的" 结果的重要差别. 例如, 1922 年提出而由 Gerd Faltings(德国数学家, 1954 年出生) 在 1983 年证明了的莫德尔猜想[V.29] 指出, 次数 $n>3$ 的光滑有理曲线上最多只有有限多个坐标为有理数的点. 在其许多推论中就有: $n\geqslant 4$ 时费马方程 $x^n+y^n=z^n$ 当最多只有有限多个整数解 (当然, 现在知道了它没有非平凡解, 但是莫德尔猜想是在费马大定理得证之前就已经证明了的, 再说这个猜想还有许多其他推论). 然而, Faltings 的证明是**无效率的**, 就是说, 它对于到底有多少个解没有给出任何信息 (只告诉人们, 解不会有无穷多个), 也没有说明解有多大, 所以也不能先用计算机来求解, 然后就说问题已经解决. 数论中有许多别的证明, 虽然重要却是无效率的, 而用有效率的证明去代替它们将是重大的突破.

对另一个未决问题的证明提出了完全不同的一类问题, 这就是四色定理[V.12], 这是德 · 摩根[VI.38] 的学生 Francis Guthrie 在 1852 年提出而由 Appel 和 Haken 在 1976 年证明的. 证明本质地应用了计算机. 他们从一个理论论证开始, 把问题化为检验有限多个特殊情况, 但是这些情况的个数如此之大, 所以不能够用人工处理, 而只能用计算机. 但是怎么来判断这个证明呢? 怎么能确定计算机的编程是正确的呢? 就算能, 对于这么大规模的计算, 怎么知道计算机的运行是正确的呢? 而一个依靠计算机的证明真正能告诉我们, 为什么这个定理为真吗? 直到今天, 这些问题还在辩论之中.

进一步阅读的文献

Archimedes. 2002. *The Works of Archimedes*. Translated by Heath T L. London: Dover. Originally published 1897. Cambridge: Cambridge University Press.

Chabert J-L, ed. 1999. *A History of Algorithms: From the Pebble to the Microchip*. Berlin: Springer.

Davies M, ed. 1965. *The Undecidable*. New York: The Raven Press.

Euclid. 1956. *The Thirteen Books of Euclid's Elements*. Translated by Heath T L (3 volumes) 2nd edn. London: Dover. Originally published 1929. Cambridge: Cambridge University Press.

Gray J J. 2000. *The Hilbert Challenge*. Oxford: Oxford University Press.

Newton I. 1969. *The Mathematical Papers of Issac Newton*. Edited by Whiteside D T,

volume 3 (1679-1673): 43-47. Cambridge: Cambridge University Press.

II.5 数学分析的严格性的发展

Tom Archibald

1. 背景

本文讨论的是严格性是怎样被介绍到数学分析里面的. 这是一个复杂的主题, 因为数学的实践已经有了相当大的变化, 特别是在从微积分的创立 (比 1700 年稍早一点) 到 20 世纪初期这一段时间里, 虽然在一定意义下, 对于什么是正确的合逻辑的论据, 基本的判据并没有变, 但是, 需要我们做这种论证的环境, 甚至在一定程度上, 做这种论证的目的, 却在随时间而改变. 1700 年代那些卷轶浩繁而又取得大成就的与约翰 · 伯努利和丹尼尔 · 伯努利[VI.18] 、欧拉[VI.19] 和拉格朗日[VI.22] 这些人相关的数学分析, 其方法的缺少基础的清晰性, 在以后的时期中, 招来了批评也得到了弥补. 到 1910 年左右, 对于如何使得数学分析中的论证严格已经出现了一般的共识.

数学所包含的不仅有计算技巧, 还有描述几何对象的重要特性的方法和世界现象的模型等等. 近来, 所有做数学研究的数学家, 都受到过如何得出严格的论证来论证自己的结论的训练, 他们也关心这些. 这些结论通常表述为**定理**, 也就是关于一些事实的命题, 同时也关心对这些命题作论证, 即证明定理为真. 下面是一个简单的例子：每一个正整数, 若能被 6 整除, 也必能被 2 整除. 沿着 6 的倍数的表往下看：$\{6,12,18,24,\cdots\}$, 就可以看到, 其中每一个数都是偶数, 这使得很容易就会相信这个命题. 关于这个命题的一个可能的论证如下：因为 6 可以被 2 整除, 所以, 每一个可以被 6 整除的数, 必定可以被 2 整除.

这样一个论证算不算一个彻底的证明, 读者可以各有看法. 因为看到这个论证以后, 可以提出这样的问题即这是否总是真的：如果 a,b,c 是三个正整数, 而且 c 可以被 b 整除, b 可以被 a 整除, 则 c 也一定可以被 a 整除吗？到底什么是整除性, 什么是整数？数学家处理这些问题的办法是：对概念作精确的定义 (例如一个数被另一个数的整除性), 把这些定义的基础放在数量有点少的未定义的名词上 (“整数”可能算一个, 但是还可能再回溯一点, 从集合开始). 例如可以定义, 所谓数 n 可以被数 m 整除, 当且仅当存在一个整数 q, 使得 $qm=n$. 利用这个定义可以给出一个更精确的证明：若 n 可被 6 整除, 则对某个 q 有 $n=6q$, 从而 $n=2\,(3q)$, 这就证明了 n 可以被 2 整除. 这样, 可利用整除性的定义来证明, 只要被 6 整除的定义成立, 则可以被 2 整除的定义也成立.

从历史来看, 数学的作者们会满足于不同水平的严格性. 数学的结果和方法时

常已经得到广泛的应用, 而没有如刚才概述地那样完全的论证, 特别是那些新的快速发展着的数学思想的总体是这样. 在有些古代文化中, 例如在埃及文化中, 已经有了乘法和除法的方法, 但是这些方法的论证则从未流传下来, 而且特别可能的是, 这种形式论证并没有存在过. 很可能是, 这些方法被接受, 只是因为它们管用, 而不是因为它们有彻底的论证.

到了 17 世纪中期, 欧洲从事研究的数学作者, 都很熟悉由欧几里得[VI.2] 的《几何原本》所提供的严格的数学论证的范本了. 那是一种演绎的, 或者说是综合的论证方法, 前面已经举例说明过, 是一种**更加几何化**(more geometrico) 的论证方法. 虽然按照今天的标准来看, 欧几里得的论据、假设和定义并不完全严格, 但基本的思想是清楚的: 从清楚的定义和所公认的基本思想 (例如全体大于部分) 出发来一步一步地导出定理 (或称命题), 而不引入任何外加的东西 (不论是狡猾地偷偷加入, 或者不知不觉地加入, 都不行). 这种几何论证的经典模型, 广泛地用于对于数论 (如费马[VI.12])、解析几何 (如笛卡儿[VI.11]) 和力学 (如伽利略) 的推理.

本文讨论的是分析中的严格性. 分析一词的意义是一直在变化着的. 它本来有古老的来源, 而到 1600 年左右, 这个词指的就是利用未知量 (现在会写成 x 的东西) 来进行计算或者求长度这一类的数学. 换言之, 它与代数有密切的关系, 虽然这个概念被笛卡儿等人输入到几何学里去了. 然而在 18 世纪的进程中, 这个词变得与微积分有关了, 而微积分成了分析技巧的应用的主要用武之地. 当谈分析中的严格性时, 主要就是讨论与微分学和积分学有关的数学的严格性. 在 17 世纪的第三个四分之一的年代, 牛顿[VI.14] 和莱布尼兹[VI.15] 为微分学和积分学制定了对立的方法, 他们就这样把相当数量的早前这两个方面的工作综合了、推广了, 这两个方面就是关于曲线的切线和法线, 还有曲线所包围的区域的面积. 这些技巧非常成功, 于是很快地就被推广到各个方向, 最值得注意的是力学和微分方程.

这项研究的共同的关键特点是无穷量的使用, 在某种意义下, 这里涉及制定一个方法来把无穷多个无穷小的量合并, 以得到有限的答案. 例如, 设把一个圆周作 (数量很大的) 等分, 就是标记出许多等距离的点, 然后把这些点连接起来, 并与圆心连接, 成为许多三角形. 这些三角形的面积之和就逼近了圆的面积, 而分点用得越多, 逼近就越好. 让我们想象有无穷多个这样内接的三角形, 每一个的面积都 "无限的小", 或者就叫做无穷小. 但是因为总体涉及把无穷多个无穷小加起来, 还是有可能得到有限的正的总量, (而不是把无穷多个零加起来仍然得到 0, 也不是把同样的有限量加无穷多次, 得到一个无穷大的数). 制定了许多做这种计算的方法, 然而对于所发生的事解释不一. 这里涉及的无穷的量是 "真正的" 无穷小, 还是只不过是 "潜在的" 无穷小①? 如果有什么东西是真正的无穷小, 那它是不是就是零呢? 亚

①就是亚里士多德的 "实无限" 和 "潜无限". —— 中译本注

里士多德学派的作者一直害怕真正的无穷小, 这方面的抱怨在那时是很普遍的.

牛顿、莱布尼兹和他们的追随者们提出了一些数学论据来证明这些做法合理, 然而引入技巧的推理是关于无穷小的对象、极限过程、无穷和等等, 这就意味着微积分的创造者们在他们的推理中是在开辟新的基础, 而由于所用的名词意义含混, 由于在作出一个结论的同时, 似乎也完全能够得到其他的结论, 这些推论的可理解性时常岌岌可危. 他们讨论的对象包括无穷小 (即比直接经验过的量无穷地小的量)、消失着的量的比 (即形如 0/0 的分数, 或者趋近于这种分数)、无限多个正量的有限和. 特别是泰勒[VI.16] 级数表示, 引起了许多这类问题. 所谓泰勒级数就是: 一个函数可以这样写成一个级数, 使得如果把这个级数就看成是函数时, 在给定的点 $x=a$ 处它会给出相同的值、相同的变率 (即一阶导数)、相同的任意阶高阶导数:

$$f(x)=f(a)+f'(a)(x-a)+\frac{1}{2}f''(a)(x-a)^2+\cdots.$$

例如, $\sin x = x - x^3/3! + x^5/5! + \cdots$, 这件事牛顿本人就已经知道, 虽然这个级数现在以牛顿的门人泰勒[VI.16] 命名.

早期的论证中还有一个问题, 就是对于所讨论的名词, 不同的作者有不同的用法. 从这种缺乏清晰性还产生了其他问题, 因为它掩盖了许多问题. 可能其中最重要的是一个论据在某个情况下失效, 而很类似的论据在另一个情况下又完全能行. 到了一定的时候, 在把分析加以推广时就会出大问题. 分析在最终还是变得完全严格了, 这些困难都解决了, 但是这个过程很漫长, 一直到 20 世纪初才完成.

下面是这种在最开始的时候就出现的困难的例子, 这是莱布尼兹的一个结果. 设有两个变量 u 和 v, 而当另一个变量 x 在变化时, 它们每一个都在变. 记 x 的无穷小变化为 $\mathrm{d}x$, 即 x 的微分. 微分是一个无穷小量, 看成一个几何量, 例如看成长度. 想象把它与其他的量按通常的方式或者组合, 或者比较 (因为两个长度可以相加, 可以有比等等). 当 x 变成 $x+\mathrm{d}x$ 时, 令 u 和 v 分别变成 $u+\mathrm{d}u$ 和 $v+\mathrm{d}v$. 莱布尼兹做出了这样的结论: uv 将要变成 $uv+u\mathrm{d}v+v\mathrm{d}u$, 所以 $\mathrm{d}(uv)=u\mathrm{d}v+v\mathrm{d}u$. 他的论据粗略地说是这样的:

$$\mathrm{d}(uv)=(u+\mathrm{d}u)(v+\mathrm{d}v)-uv,$$

把右方按照正规的代数展开、化简, 会给出 $\mathrm{d}(uv)=u\mathrm{d}v+v\mathrm{d}u+\mathrm{d}u\mathrm{d}v$. 但是 $\mathrm{d}u\mathrm{d}v$ 这一项是二阶无穷小, 比起一阶无穷小来说是消失的小 (vanishingly small), [用现代语言来说就是高阶的小量], 所以可以作为 0 来处理. 说真的, 这里的问题有一个侧面, 就是在处理无穷小时出现了**不相容**的情况. 再例如, 如果想求出 $y=x^2$ 的导数, 这里的计算正相应于上面的计算 (把 $(x+\mathrm{d}x)^2$ 展开等等), 得到 $\mathrm{d}y/\mathrm{d}x=2x+\mathrm{d}x$. 然后, 把右方的 $\mathrm{d}x$ 当作 0 来处理, 而左方的 $\mathrm{d}x$ 又似乎是看作无穷小的非零量, 因

为不然就不能用它来作除数. 所以, 它是零还是非零? 如果不是, 又怎么绕过这里的明显的不相容性?

在稍微更加技术性的层次上, 微积分要求数学家一再地处理当分子和分母都趋近 0 甚或真正为 0 时, 形如 dy/dx 的比的 "最终值" 问题. 在我们的陈述里, 又一次使用了莱布尼兹的微分记号, 虽然对于牛顿也发生了同样的问题, 不过记号与概念上稍有区别. 当牛顿讲到变量时, 他总认为变量是依赖于时间的, 例如他力求考虑在消逝 (evanescent) 的量 —— 就是消失地小的增量下 [变量] 所趋近的值. 一组无法消除的混淆正是来自这样一个思想, 即变量是处在变化过程中, 不论是随时间变化或者随其他变量而变化. 这就是说, 我们考虑的是趋近一个给定的值的变量所取的值, 但对于究竟什么叫 "趋近" 又没有一个清晰的概念.

2. 18 世纪的处理方法以及对它的批判

当然, 如果微积分没有成为成就巨大的研究领域, 就谁也不会来操心批判它了. 但是, 牛顿和莱布尼兹的方法被广泛地应用来解决前代人感兴趣的问题 (最值得注意的有切线和面积问题), 而在提出和解决问题上, 那些技巧突然变得容易接受多了. 面积问题、极大极小问题、描述悬挂着的链子的形状 (即悬链线) 或者振动着的弦上的点的位置的微分方程的提出和求解, 对于天体力学的应用, 以及与函数性质有关的研究 (虽然这里讲的函数, 在绝大多数的情况下是指含变量的表达式)—— 所有这些领域还有其他领域在整个 18 世纪都在发展, 这是由泰勒、约翰 · 伯努利和丹尼尔· 伯努利、欧拉、达朗贝尔[VI.20]、拉格朗日还有许多别人的贡献. 这些人使用了许多大师般的论证的绝技, 但是这些论证的有效性又多有可疑之处. 在这些大师们中最杰出的人物手上, 对于发散级数进行运算、虚数的应用、涉及实无穷的操作, 用得真是得之于心、应之于手. 然而这些方法, 对于不如大师们那么出色的人, 又总是很难解释清楚, 所以有些结果再重复起来就不太可靠了 —— 从今天的观点看来这真是怪事. 要做欧拉的计算, 您就得自己就是欧拉, 这种情况延续到了下一个世纪.

一些特定的争论突出了一些问题, 而今天看来这些问题是来自基础上的混淆不清. 例如, 在无穷级数问题上, 就有着形式表达式的适用范围上的混淆. 考虑级数

$$1-1+1-1+1-1+1-\cdots.$$

按照今天通用的初等定义 (这是柯西[VI.29] 在 1820 年左右提出的), 将把这个级数考虑为发散级数, 因为它的部分和序列 $1,0,1,0,\cdots$ 不趋向任何极限, 但是关于这个式子却有争论. 例如欧拉和尼科拉斯 · 伯努利就讨论过, 一个无穷和的**和**与**值**可能有区别, 伯努利认为, 像 $1-2+6-24+120+\cdots$ 这样的东西并没有**和**, 但是这个代数表达式可以有**值**. 欧拉则为下面的观念辩护说, 级数的**和**就是产生这个级数的有限表达式的**值**, 也不管这些名词究竟是什么意思. 在他的 1755 年的 *Institutiones*

Calculi Differentialis 一书里, 他以 $1-x+x^2-x^3+\cdots$ 为例. 这个式子是由 $1/(1+x)$ 得来的, 所以后来欧拉在为自己的观点辩护时, 就说 $1-1+1-1+\cdots=1/2$. 他的观点并未得到普遍接受. 在把函数的值推到其通常的区域以外时, 例如对于负数的对数, 也产生过类似的争论.

对于 18 世纪的分析的语言和方法的最著名的 18 世纪批评家大概就是哲学家贝克莱 (George Berkeley, 1685–1753, 爱尔兰哲学家, Cloyne 地方的主教). 他的名言"存在即被感知"表明了他的唯心主义立场, 同时还加上他的强烈的信念, 即对个别的品质作抽象以供哲学的讨论是不可能的. 所以, 这些的对象应该是被感知的东西, 而且应该是作为一个整体而被感知的. 感知无穷小的大小的物体的不可能性, 再加上它的明显的抽象本性, 使得贝克莱在他 1734 年出版的著作《分析学家: 或致一位不信神的数学家的信》(*The Analyst: Or, a Discourse Addressed to an Infidel Mathematician*) 里讥讽地称无穷小为"消逝的量的鬼魂", 他的辩词是: 在数学论证里, 忽略去一个量, 不论它多么小, 都是不合适的. 他引用了牛顿关于这个问题的话: "在数学中, 哪怕是最小的误差, 也是不许可的." 贝克莱接下去又说, 正是这门学科的晦涩使得牛顿把这类推理强加于他的追随者. 这样一些评论, 虽然明显地并不能阻止那些倾心于这个方法的人, 但确实增强了这样一种感情, 认为微积分的这一个侧面确需更深入的解释. 如欧拉、达朗贝尔、老卡诺[①]等和其他人就企图通过澄清微分是什么来回应对于基础的批评, 并且作了许多论证来说明微积分的运算是正当的.

2.1 欧拉

欧拉对于分析的一般发展所作的贡献多于 18 世纪的任何人, 他为了论证他的方法所给出的论据, 由于他所写的重要的教科书的成功与被广泛采用, 甚至在他身后仍然有极大的影响. 欧拉的推理有时被认为是很不严谨, 因为用起微积分记号来很是随心所欲, 他的许多论证按后来的标准看也都是有缺陷的. 特别当这些论证涉及无穷级数和无穷乘积时更是如此. 一个典型的例子是他对以下式子的早期的证明:

$$\sum_{n=1}^{\infty}\frac{1}{n^2}=\frac{\pi^2}{6}.$$

他的方法是这样的, 利用 $\sin x$ 的已知级数展开式

$$\frac{\sin\sqrt{x}}{\sqrt{x}}=1-\frac{x}{3!}+\frac{x^2}{5!}-\frac{x^3}{7!}+\cdots,$$

①科学史上有两位卡诺, 这一位是 Lazare Nicolas Maguérite Carnot, 1753–1824, 法国数学家, 另一位是他的儿子 Sadi Nicolas Léonard Carnot, 1796–1832, 是物理学家, 以热力学的奠基者之一而著称于世. —— 中译本注

欧拉考虑左式的零点, 其位置在 $\pi^2, (2\pi)^2, (3\pi)^2, \cdots$ 等处, 应用适用于有限代数方程的因式定理 (而对此未作任何论证), 他把这个式子写成①

$$\left(1-\frac{x}{\pi^2}\right)\left(1-\frac{x}{4\pi^2}\right)\left(1-\frac{x}{9\pi^2}\right)\cdots=\frac{\sin\sqrt{x}}{\sqrt{x}}.$$

现在可以看到, 双方 x 的系数应该相等. 右式的系数是 $-1/6$, 而欧拉把左方各个括号都乘开, 其中除了一个括号外都取 1, 这一项则取 $-x/k^2\pi^2$. 这样欧拉得到

$$\frac{1}{\pi^2}+\frac{1}{4\pi^2}+\frac{1}{9\pi^2}+\cdots=\frac{1}{6}.$$

双方乘以 π^2 即得所求证明的式子.

我们现在认为这个处理途径有几个问题. 无穷多个因子的乘积可能表示一个有限值, 也可能不表示, 今天就会要求确定它何时才表示一个有限值. 还有把适用于 (有限) 多项式的结果用于无穷级数, 是需要论证的步骤. 欧拉在他的晚年对此结果给出另一个论证. 他可能已经知道有反例一说 —— 即这种用法可能不行的情况 —— 但是, 这样的事实, 对于欧拉却不是决定性的障碍. 这样的观点, 即在一般能行而可能有少数例外的情况下, 仍然进行推理, 在欧拉的时代并不少见, 直到 19 世纪末, 人们才通过协调的努力做到了这样的地步 [即达到了这样的共识]: 在宣布分析的结果时, 要确切地阐明这个定理成立的条件.

欧拉并没有细想过如何解释无穷和以及无穷小. 有时, 他轻率地就把无穷小当作真正为零, 而且从问题的上下文来导出微分之比的意义:

> 一个无穷小的量无非就是一个正在消逝的量, 所以, 将会真正变成零 …… 所以在这个概念后面, 和通常的想法不一样, 并没有什么神秘的东西. 这种假设的神秘使得无穷小的计算对于许多人变得很为可疑.

这个声明见于欧拉 1755 年写的 *Institutiones Calculi Differentialis* 一书, 紧接着他就来讨论在比例中有一个比②为 0/0 的问题, 这样来论证在普通的数的计算中微分可以略去. 这个声明很准确地描述了欧拉的实践的很大一部分 —— 例如他在研究微分方程时就是这样做的.

然而, 确实发生了冲突的事, 而关于定义的辩论也不少见. 最著名的例子涉及关于所谓振动弦问题的讨论. 欧拉、达朗贝尔和丹尼尔 · 伯努利都卷进来了. 这些辩论紧密地关乎函数[I.2 §2.2] 的定义, 以及在分析中所研究的函数有哪些可以用级数 (特别是三角级数) 来表示的问题. 一条形状任意的曲线都可用作振动弦的初

①原书此式右方误为 0. —— 中译本注

②比和比例其实是初等数学里的问题. 当我们说两个数的比 $a:b$ 时, 实际上就是说的分数 a/b. 不过用分数记号时需要避免分母为 0 出现, 但在讲到比的时候, 并不限制后项 (即 b) 不能为零. 这可能是因为古代人们对分母不得为 0 不如现代人那么敏感. 比例就是多个比相等, 例如: $a:b=c:d$(即 $a/b=c/d$). 所以正文中说到 "比例中有一个比为 0/0" 这样的话. —— 中译本注

始位置, 这样的思想推广了函数的思想, 而傅里叶[VI.25] 在 19 世纪早期的工作又使得这些函数在解析上可以处理. 在这样的背景下, 具有折断的图像的函数 (一类**不连续函数**) 就被纳入人们的视线了. 后来, 当与代数和三角运算相联系的 "更自然" 的对象让位于更一般的现代的函数概念时, 如何对待这类函数, 成了分析基础的决定性的问题.

2.2 18 世纪晚期的回应

在英国, 对于贝克莱的一个值得注意的反应来自麦克劳林 (Colin Maclaurin, 1698–1746, 苏格兰数学家), 他在 1742 年写的教本《论流数》(*A Treatise of Fluxion*) 试图澄清微积分的基础, 消除掉无穷小量. 麦克劳林是 18 世纪中叶所谓苏格兰启蒙时期的领导人物之一①, 是当时最出色的英国数学家, 是牛顿的方法的热忱拥护者. 他的著作, 在欧洲大陆, 和当时许多英国同时代人的著作不一样, 得到了人们的阅读和兴趣, 特别是他对牛顿天体力学的详细解释. 麦克劳林企图用所谓 "可指定的" 有限量的极限这一概念作为他的推理的基础. 麦克劳林的著作虽然确实给出了计算比的极限的例子, 却是以晦涩著称的. 他对于澄清分析基础的最大的贡献可能在于他对达朗贝尔的影响.

达朗贝尔读过贝克莱和麦克劳林的著作, 而在拒绝无穷小量这一点上追随他们二人. 当他探讨微分作为极限这个思想时, 也企图把自己的思想与无穷小量可以无矛盾地看作是真正的零的思想调和起来, 说不定这是对欧拉的思想的一种首肯. 关于达朗贝尔的观点的主要作品可以在他主编的《百科全书》(*Encyclopédie*) 中关于微分的文章 (1754 年发表) 和关于极限的文章 (1765 年) 中找到. 达朗贝尔为几何极限辩护, 认为它比代数极限更重要. 他的意思似乎是, 对于所研究的量, 不能仅仅作形式的研究, 就是不能仅仅用代换和简化来研究. 极限可以说是长度 (或许多长度) 的极限、面积的极限, 或者其他有维度的量的极限, 正好像把圆看成内接多边形的极限那样. 他的目的似乎主要在于确立由现存的算法来描述的对象的现实性, 因为他实际运用的计算是用微分来进行的.

2.2.1 拉格朗日

在整个 18 世纪里, 微分学和积分学逐渐从它们对力学和物理学的应用中独立出来, 成为一整套方法. 同时, 这些方法的焦点也从几何学移开, 所以在 18 世纪后半叶我们越来越多地看到, 微积分被处理为 "解析函数" 的 "代数分析". "解析" 这个词在多种意义下使用. 对于许多作者, 例如欧拉, 解析只不过就是讲的函数 (作为变量之间的关系), 即用分析中常用的单个表达式来表示的函数.

拉格朗日依据这种代数的观点为微积分提供了一个基础. 拉格朗日集中注意

①这是指 1740–1790 年代. 当时在苏格兰涌现了一大批思想家和科学家, 例如有大卫 · 休姆、亚当 · 斯密等等. —— 中译本注

于幂级数展开式, 把它作为分析的基本实体, 通过他的工作, 解析函数这个词向着它的比较现代的意义演化, 即与收敛的泰勒级数展开式相联系. 他的途径在他 1797 年的《解析函数论》(*Théorie des Fonctions Analytiques*) 一书里得到充分的表现. 此书是他在巴黎高工讲义的一个版本, 而高工是当时为革命的法国训练军事工程师的精英的新机构. 拉格朗日假设一个函数一定能表示为代数函数的无穷级数, 他的这个论证是以已知的函数展开式的存在为基础的. 他先是努力来证明在这个表达式里,"一般说来" 不会有负幂和分数幂出现, 由此他就得到了一个幂级数表达式. 他的论据在这里有些令人惊奇, 多少有点 ad hoc, [即为此目的而人为造作的], 我现在用 (Fraser, 1987) 一文中给的例子 [来说明拉格朗日的方法]. 这里的有点奇怪的记号是以拉格朗日的记号为基础的. 设想要找出函数 $f(x)=\sqrt{x+i}$ 用 i 的幂的表达式. 一般说来这里只会出现 i 的整数幂, 因为, 拉格朗日说, $i^{m/n}$ 这种形式的项是没有意义的, 函数 $\sqrt{x+i}$ 的表达式只有两个值, 而 $i^{m/n}$ 有 n 个值, 而级数

$$\sqrt{x+i}=\sqrt{x}+pi+qi^2+\cdots+ti^k+\cdots$$

可以从 $\sqrt{x}$ 得到两个值, 因此其他的项必定是 i 的正整数幂. 把分数幂撇开以后, 拉格朗日就论证说 $f(x+i)=f(x)+i^aP(x,i)$, 其中的 P 当 $i=0$ 时是有限的. 继续应用这个结果得到以下的表达式:

$$f(x+i)=f(x)+pi+qi^2+ri^3+\cdots,$$

这里 i 是一个小的增量. 数 p 也依赖于 x, 所以拉格朗日就定义它为 $f(x)$ 的导函数, 记作 $p(x)=f'(x)$. 导函数或英文的 derivative, 其中的 "导" 字, 来自法文的 dérivée, 就是导出的意思, 而按照拉格朗日的用语, $f(x)$ 就是导函数的 "原函数". 类似的论据可以把高次的系数与通常的泰勒级数中的高阶导数联系起来.

以今天的眼光看来, 拉格朗日的途径奇怪地有点循环论证的味儿, 这是因为在 18 世纪把级数的 "代数" 无限过程与使用微分是区别开来的. 拉格朗日并没有看到, 原来的级数展开式就是以极限过程为基础的. 由于重新强调极限, 以及由柯西发展起来的新定义, 拉格朗日的这个途径很快就被看成是站不住脚的了.

3. 19 世纪的前半世纪

3.1 柯西

在 19 世纪第一个十年中, 对于分析中的严格性有贡献的作者很多. 但是, 柯西第一个重新恢复了极限的途径, 而取得了最大的效果. 他是出于教学的目的, 他的思想可能是在 1820 年代初为巴黎高工准备入门课程时提出来的. 虽然那里的学生在学术能力上是全法国最好的, 许多学生仍认为他的讲法太难. 结果, 一方面柯西仍然按自己的方法讲课, 而其他教师则按老的无穷小量的讲法, 因为他们觉得那样

的讲法对于学生直观而易于接受, 对解决初等力学问题也更适合. 1830 年代, 柯西自行流放离开巴黎, [实际上是因为反对当时的政府而逃到意大利去了], 更限制了他的讲法的影响, 而这种讲法本来就只有少数学生接受.

虽然如此, 柯西关于极限、连续性和导数的定义在法国还是逐渐得到普遍采用, 在其他地方, 特别是意大利也是如此. 此外, 他在证明中使用这些定义, 特别是使用各种形式下的中值定理, 这样一些方法, 使得分析不再是对一些具有特殊性质的量 [即指无穷小量] 的符号操作, 而成为利用不等式的操作作精密的估计这样一种研究无限过程的科学.

在某些方面, 可以说柯西的最大贡献在于他的清晰的定义. 对于早前的作者, 无穷级数的和是一个多少有点模糊的概念, 有时可以用一种收敛性的论据来解释 (例如在几何级数 $\sum_{n=0}^{\infty} 2^{-n}$ 的情况), 有时又作为此级数所来自的函数的值来对待 (如欧拉就时常这样做). 柯西对定义这样来修改, 宣称无穷级数的和就是其部分和序列的极限. 这样做, 对于数项级数和函数项级数提出了统一的处理途径. 这是把微积分和分析的基础移到以实数概念为基础的重要一步. 这个潮流最终占了统治地位, 时常被称作是 “分析的算术化”. 类似于此, 现在连续函数就是具有以下性质的函数: “变量的无穷小增加导致函数本身的无穷小增加” (Cauchy, 1821: 34-35).

上面的例子说明, 柯西并没有躲着无穷小走, 他也没有对无穷小作进一步的分析. 他对极限的定义, 现在看来是一种对话式、启发式的 (Cauchy, 1821: 4):

> 若对于一个变量所指定的值, 无限地趋近于一个确定的值, 使得它与此值之差变得想要多小就有多小, 这个确定的值就称为所有其他值的**极限**. 这样, 举例来说, 一个无理数就是许多分数的极限, 这些分数给出的值离此无理数越来越近.

这些思想按现在的标准来看并不完全严格, 但是柯西可以用它给分析里的种种基本过程以统一的基础.

对于无穷小量的应用, 例如就出现在他对连续函数的定义里. 为了揭示这个定义, 设有一个函数 $f(x)$ 定义在实数直线的某一个有限区间上, 而且是单值的, 然后在此区间里任取一值 x_0. 如果把这个值增加为 x_0+a, 则函数值也会改变一个量 $f(x_0+a)-f(x_0)$. 如果对此区间里的任意 x_0, $f(x_0+a)-f(x_0)$ 与 a 同时无限地趋近于 0, 柯西就说这个函数在此区间上是连续的. 换句话说, 柯西定义的连续性是在一个区间上, 而不是在一点处的性质, 本质上就是说, 在此区间上自变量的无穷小变化产生函数值的无穷小变化. 柯西是把连续性考虑为函数在一个区间上的性质的.

这个定义强调了函数值的跳跃对于理解这个函数的重要性, 这一点柯西在他早前研究微积分的基本定理[I.3 §5.5] 时就遇到过. 柯西在 1814 年关于定积分的论文中就说过 (Oeuvres, volume Ⅰ: 402-403):

若函数 $\phi(z)$ 在 $z=b'$ 和 $z=b''$ 以连续的方式增加或减少, 则积分 $\left[\int_{b'}^{b''}\phi'(z)\,\mathrm{d}z\right]$ 通常可以表示为 $\phi(b'')-\phi(b')$. 但是, 若 …… 函数突然地从一个值跳到另一个明显不同的值 …… 则积分的通常的值必须减少.

柯西在他的讲义里定义定积分时, 假定了连续性. 他首先考虑把积分区间分成有限多个子区间, 而在每一个子区间上函数或上升或下降 (这件事并非对每一个函数都可以做到, 但是看来这没有使柯西操心). 然后, 他就定义定积分为以下的和的极限: $S=(x_1-x_0)f(x_0)+(x_2-x_1)f(x_1)+\cdots+(X-x_{n-1})f(x_{n-1})$ 当数 n 变得很大时的极限. 柯西用关于中值的定理和连续性的事实, 对于极限的存在给了详细的论证.

柯西的讲义的主要科目的各个版本在 1821 年和 1823 年出版, 后来, 高工的每一个学生都知道这些讲义, 而许多人则公开地用过. 其后在 1841 年, 又由柯西的合作者莫瓦尼奥神父①写了详加解释的版本. 它们在法国常被引用, 而由柯西使用的定义, 后来在法国成了标准. 我们还知道, 许多其他人也研读过这些讲义, 其中著名的有阿贝尔[VI.33] 和狄利克雷[VI.36], 他们在 1820 年代都在巴黎待过, 黎曼[VI.49] 也读过这些讲义.

柯西离开了拉格朗日的形式化途径, 排斥了 "代数的模糊性". 虽然柯西是受到直觉 (几何直觉和其他直觉) 的指引, 他清楚地知道直觉有时会引人进入歧途, 并且举了一些例子说明紧贴准确的定义的价值. 其中一个著名的例子就是给出了一个函数: 当 $x\neq 0$ 时, 其值为 e^{-1/x^2}, 而当 $x=0$ 时, 其值为 0, 这个函数可以微分无穷多次, 然而其泰勒级数却不收敛于此函数. 尽管柯西给出了这个例子, 而且在自己的讲义中讲到它, 柯西却不是反例的专家, 事实上, 通过反例来澄清定义这个潮流还是后来的发展.

阿贝尔干了一件使他非常出名的事情, 他使人注意到柯西工作中的一个错误, 这就是柯西声称一个收敛的连续函数级数必有连续的和, 而在 1826 年, 阿贝尔给出以下级数作为反例:

$$\sum_{k=1}^{\infty}(-1)^{k+1}\frac{\sin kx}{k},$$

它在 π 的奇数倍处是不连续的. 柯西只是在后来好几位作者都指出这个现象以后, 才 [明白了收敛与一致收敛] 的区别. 历史学家们关于这个错误写过许多文章, 其中

①莫瓦尼奥 (Abbé Francois Napoleon Marie Moigno), 1804–1880, 柯西的朋友, 耶稣会教士. 当时的耶稣会要求它的教士们把传教与科学文化活动结合起来. 例如把欧几里得《几何原本》传播到中国的利玛窦就也是耶稣会的教士, 他在中国的活动也是按这个原则进行的. 莫瓦尼奥不只与柯西有密切的来往, 还与当时法国的著名科学家安培、作家大仲马有密切来往. 正文中说到的版本, 就名为《微积分教程 (按照柯西手稿)》(*Leçons sur les Calcul Differentiel et Integrale, (d'après Cauchy)*), 1840–1844. —— 中译本注

有一篇 Bottazini 的文章颇有影响, 提出由好多柯西并不认为阿贝尔的例子有效的理由, 看来柯西当时就已经知道这个例子 (此文可见 (Bottazini, 1990: LXXXV)).

在离开柯西以前, 我们还要提一下*波尔扎诺*[VI.28] 与此相关的独立的活动. 波尔扎诺 (Bernard Bolzano, 1781–1848, 是一位波希米亚的天主教教士、数学家, 波希米亚就是现在的捷克) 的思想在当时并未得到广泛传播, 他广泛地研究了微积分的基础. 例如, 1817 年他写了一篇文章, [题目很长, 叫做 "**以下定理的纯粹解析证明, 若函数在两点取任意的反号的值, 则在其间必有方程至少一个实根存在**"], 其实就是中间值定理. 他也研究过无穷集合, 现在所说的波尔扎诺–魏尔斯特拉斯定理指出, 每一个有界无穷集合至少有一个点具有以下性质: 围绕此点的任意球体必包含此集合的无穷多个点. 这种 "极限点" 由*魏尔斯特拉斯*[VI.44] 独立地研究过. 到了 1870 年代, 波尔扎诺就更加为人所知了.

3.2　黎曼, 积分和反例

黎曼由于以他命名的黎曼积分而与分析的基础不可分地联系起来了. 这个积分已经是每一个微积分课程的一部分了. 尽管如此, 他并不总是受到有关严格性的问题所驱动的. 事实上, 他一直是非严格的直觉发明会带来丰硕成果的标准的例子. 黎曼的工作中有许多地方很自然地会引起严格性问题, 他的创造性的广阔的兴趣, 极大地引导着研究者把他的这些洞察力精确化.

黎曼的定积分定义见于他在 1854 年的就职论文①——"第二篇博士论文", 这篇论文使他取得了在大学里担任有酬劳的讲师的资格. 在这篇文章里, 黎曼把柯西的概念推广到函数不一定连续的情况. 他做这个工作是作为他对*傅里叶级数展开式*[III.27] 的研究的一部分. 这种级数的广泛的理论是由傅里叶在 1807 年给出, 但是到 1820 年代才发表的. 傅里叶级数把一个函数在一个有限区间上写成以下的级数形式:

$$f(x) = a_0 + \sum_{n=1}^{\infty} (a_n \cos nx + b_n \sin nx).$$

黎曼的工作的直接灵感来自*狄利克雷*[VI.36], 狄利克雷改正了柯西在函数的傅里叶级数展开何时收敛又是否收敛于它所来自的函数这个问题上的毛病. 1829 年

①按照当时德国的制度, 得到博士学位后想在大学任教, 一定要做一个就职演说 (habilitationsvortrage), 交一篇就职论文 (habilitationschrift). 演说和论文的题目是 "竞争上岗者" 自己提出, 再由博士导师 (黎曼的导师就是高斯) 指定. 黎曼提出了三个题目, 第一个就是这里讲的关于三角级数的 "论函数值可以表示为三角级数", 黎曼自己最希望讲的就是这一篇, 但是高斯选择了黎曼最不想讲的关于几何基础的一篇. 据说高斯很想听一听对于这个极为深刻的问题, 年轻人如黎曼能够讲些什么. 请参看本书 [II.2 §8]. 附带提一下, 黎曼的博士论文是关于复变函数的, 详见本书 [VI.49]. 三篇论文奠定了三门学科的基础, 这实在不能不给人 "高山仰止" 的感觉. —— 中译本注

狄利克雷证明了若一个函数以 2π 为周期, 在一个如此长度的区间上可积分, 而且没有无穷多个极大与极小, 则其傅里叶级数收敛于它, 但在间断点上则收敛于来自两侧的两个极限值的平均值. 正如黎曼追随他的导师狄利克雷说的那样, "这个主题与无穷小计算有最密切的联系, 因此可以用于把无穷小计算搞得更清晰与确定"(Riemann, 1854: 238). 黎曼想把狄利克雷的研究作进一步推广, 因此被引到对于狄利克雷的每一个条件都作详细研究, 这样, 他就把定积分的概念推广如下:

我们在 a 与 b 之间取一串上升的值 $x_1, x_2, \cdots, x_{n-1}$, 而且为简单计, 记 $x_1 - a$ 为 $\delta_1, x_2 - x_1$ 为 $\delta_2, \cdots, b - x_{n-1}$ 为 δ_n, 用 ε 表示适当的分数. 于是

$$S = \delta_1 f(a+\varepsilon_1\delta_1) + \delta_2 f(x_1+\varepsilon_2\delta_2) + \delta_3 f(x_2+\varepsilon_3\delta_3) + \cdots + \delta_n f(x_{n-1}+\varepsilon_n\delta_n)$$

之值依赖于区间长 δ 与量 ε 的选择. 如果它有以下的性质, 即不论 δ 和 ε 如何选择, 当 δ 变为无穷小时, S 都无穷地趋近于同一个固定值 A, 我们就说此值为积分 $\int_a^b f(x)\,\mathrm{d}x$.

部分地是与积分的这个定义相关, 部分地是为了说明这个定义的力量, 黎曼给出了在任意区间上都不连续但仍然可积的函数的例子. 这样, 积分在每一个区间中均有不可微分的点. 黎曼的定义就这样使得微分与积分的互逆性质也成了问题, 他的例子就把这件事大白于天下了. 到了这个时候, 这种 "病态的" 反例在推进严格性上面的作用, 虽然在柯西那里已经可以见到, 现在更是大大加强了.

黎曼的定义是在他 1866 年去世后的 1867 年发表的, 1873 年由达布 (Jean Gaston Darboux, 1843–1917, 法国数学家) 写了解说并以法文发表. 黎曼的途径的普及与推广是与人们越来越领会到严格性的重要性同步前进的, 而这又是与下面将要讨论的魏尔斯特拉斯学派相关的. 黎曼的途径集中注意于不连续点的集合, 所以又是康托[VI.54] 在 1870 年代以后有极限点的集合的种子.

狄利克雷原理的应用可以看成是黎曼的工作引起对分析基础的关注的进一步的例子. 与他对于复分析的研究相关, 黎曼被引到研究所谓**狄利克雷问题**的求解, 这就是: 给定一个函数 g 定义在一个平面闭区域的边缘上, 是否存在一个函数 f, 在区域的内域满足拉普拉斯偏微分方程[I.3 §5.4], 而在边缘上取 g 同样的值? 黎曼断定答案为是. 为了证明这一点, 黎曼把这个问题化为证明存在一个函数, 使定义在次区域上的一个积分最小化, 而且在物理学的基础上论证这个最小化函数一定存在. 甚至当黎曼还在世时, 魏尔斯特拉斯[VI.44] 就对此提出了质疑, 并且在 1870 年 [(其时黎曼已去世 4 年)] 发表了一个反例. 这就导致了许多其他数学家重新来陈述黎曼的结果, 并用其他方法给以证明, 最终, 在精确而广泛的条件下恢复了狄利克雷原理的适用性, 是由希尔伯特[VI.63] 在 1900 年给出的.

4. 魏尔斯特拉斯及其学派

魏尔斯特拉斯在学生时代在波恩和闵斯特读书时就对数学怀着热忱, 但是他的学生生涯很不平坦. 他在 1840 年到 1856 年都在担任中学教师, 独自一人研究数学, 文章都发表在人所不知的刊物上. 从 1854 年起, 他开始在《纯粹与应用数学杂志》(*Journal für die Reine und Angewandte Mathematik*)(通常又称为 *Crelle* 杂志) 上发表论文, 这才引起世人对他的才能的注目, 而在 1856 年在柏林得到了教授职务. 魏尔斯特拉斯于是开始正规地教分析课程, 他对这门学科的处理方法形成了四门课程的讲义, 这四门课他在 1860 年代早期和 1890 年代循环地开设. 随着时间演进, 这些课程有许多重要的数学家都听过. 他们又通过把未发表的讲稿非正式地流通, 从而间接地影响了许多其他人. 这一个圈子就包括了利普希兹 (Rudolph Otto Sigismund Lipschitz, 1832–1903, 德国数学家)、杜 · 波瓦 · 雷蒙 (Paul David Gustav du Bois-Reymond, 1831–1899, 德国数学家)、施瓦兹 (Hermann Amandus Schwarz, 1843–1921, 德国数学家)、赫尔德 (Otto Ludwig Hölder, 1859–1937, 德国数学家)、康托、柯尼希贝格尔 (Leo Koenigsberger, 1837–1921, 德国数学家)、米塔格–莱夫勒 (Magnus Gösta Mittag-Leffler, 1846–1927, 瑞典数学家)、柯瓦列夫斯卡娅[VI.59] 和富克斯 (Immanuel Lazarus Fuchs , 1833–1902, 德国数学家), 这里只提出其中最重要最为人知的几位. 他们通过在自己的研究中采用魏尔斯特拉斯的方法, 在自己的教学中拥护他的思想, 使得他的讲义在晚年终于出版以前很长时间, 这种方法就已经为人采用了. 以下的叙述很大程度上是基于这些讲义的 1878 年的版本. 他的方法在德国以外也很有影响, 例如其中一部分在法国就被吸收进厄尔米特[VI.47] 和约当[VI.52] 的讲义里去了.

魏尔斯特拉斯的方法是建立在柯西的方法的基础上的 (虽然这两大块知识的相互关系从来没有被充分地检验过). 魏尔斯特拉斯的方法有两个非常重要的主题: 一是在极限过程中, 消除了运动的概念, 或量的正在变化中的值的概念; 二是函数特别是复变量函数的表示. 这两个主题是密切相关的. 在极限的非运动的定义中, 魏尔斯特拉斯新创的现在称为实直线和复平面的拓扑学的研究至关重要, 在其中我们有了极限点的概念, 有了局部和整体的明确的区别. 魏尔斯特拉斯研究的中心对象是函数 (一个或多个实或复变量的函数), 但是应该注意, 并没有涉及集合理论, 所以函数**并没有**被看成有序数对的集合.

这些讲义从现在已经很熟悉的主题开始: 从整数到有理数、复数和实数的发展. 例如负数是用运算来定义的, 使得整数在减法运算下也是闭合的. 他曾经企图用统一的方法来定义有理数和无理数, 其中包括单位分数和十进小数, 但现在看来有些模糊. 魏尔斯特拉斯对于实数的定义用现代的眼光来看是不能满意的, 但是分析的**算术化**的一般道路已经由这个方法确定了. 平行于对于数系的发展, 他也发展

了函数类, 即利用幂级数表示, 从有理函数开始来建立起函数类. 这样, 按照魏尔斯特拉斯的方法, 多项式 (称为整有理函数) 被推广为"具有整数特性的函数", 就是其幂级数展开式处处收敛的函数, [就是现在说的整函数]. 魏尔斯特拉斯的因子定理断言, 任意这种函数都可以分解为某些"素"函数和具有某一类多项式指数的指数函数的乘积 (可能是无穷乘积).

魏尔斯特拉斯给出的极限定义具有彻底的现代特性①(Weierstrss, 1988: 57):

> 说变量 y 随另一个变量 x 同时变为无穷小, 就是说,"在假设了一个任意小的量 ε 后, 可以对 x 找到一个界限 δ, 使得对于每一个适合 $|x| < \delta$ 的 x, $|y|$ 的相应值必小于 ε".

魏尔斯特拉斯立即用这个定义来证明多变量的有理函数的连续性, 其论据可以在今天的教科书上找到. 变量趋于一确定值的以往的概念, 被关于互相联系的不等式的量化的命题所取代. 把各种假设放进使用不等式的框架里来陈述, 成了魏尔斯特拉斯学派的著作的指导主题. 这种语言给予例如涉及到极限的交换这类问题的清晰性, 意味着以前无法处理的问题现在可以用一种魏尔斯特拉斯学派所谆谆教导的常规方式来处理了.

一般函数都可以从有理函数用级数展开式来构造, 这个事实使得有理函数在魏尔斯特拉斯的方法里起了关键作用, 早在 1841 年魏尔斯特拉斯就确认了一致收敛性的重要. 一致收敛和逐点收敛的区别, 在魏尔斯特拉斯的讲义里面十分清楚. 关于级数的收敛性, 他和柯西一样, 是指部分和序列的收敛, 但是收敛性现在要这样来陈述: 级数 $\sum f_n(x)$ 在 $x = x_0$ 处收敛于 s_0, 如果给出任意正的 ε, 必有一个正整数 N, 使得对于每一个 $n > N$ 都有

$$|s_0 - (f_1(x_0) + f_2(x_0) + \cdots + f_n(x_0))| < \varepsilon.$$

在变量的一个区域里的一致收敛性, 则是说, 对于这个 ε, 同样的 N 对于区域中的所有 x 都管用. 一致收敛性能保证和的连续性, 因为这些级数都是有理的从而是连续的函数的级数. 从这个观点看来, 一致收敛性的重要性远超出三角级数的范围 (虽然三角级数也很重要). 事实上, 它是整个函数理论的中心工具.

魏尔斯特拉斯成了其他人 (特别著名的有黎曼) 的工作是否严格的评判者. 他的这个作用前面已经提出过了. 他所给出的反例, 用来说明已经被接受的概念的困难和区别不同的解析性态, 其数量比任何领袖人物都多. 他的最有名的例子之一, 就是造出了一个处处连续而又无处可微的函数, 这就是级数 $f(x) = \sum b^n \cos(a^n x)$. 它当 $|b| < 1$ 时一致收敛, 但当 $ab > 1 + 3\pi/2$ 时, 在任一点 x 都不可微. 类似地, 他还造出了使狄利克雷原理失败的函数的例子, 还有"自然边界", 即继续拓展级数

①这里有一点文字修改. —— 中译本注

到更大的区域去的障碍, 等等. 他鼓励做细心的区分, 以及他寻求病态而非常态的例子的过程本身, 聚焦到使得分析中的假设的精确性到了前所未有的程度. 从 1880 年代以后, 随着这个方法的成熟, 分析不再处理只是大体上能行的情况, 相反, 寻求命题的绝对的精确性, 使得这些命题的绝大多数一直到现在还能用. 它也成了数学的其他领域的典范和必定的要求, 虽然有时从一般能行的例子到表述完全的假设和定义, 有时要花上几十年 (代数几何学就是一个著名的例子, 在这个领域里, 直到 1920 年代还是在处理一般能行的例子). 在这个意义下, 魏尔斯特拉斯和他的学派所支持的严格论证和解说成了数学的一般的模式.

4.1 魏尔斯特拉斯和黎曼的影响

分析以其严格性成了各个子学科的典范, 有好几个理由. 分析仅以其结果的应用的数量之多与范围之广而言, 就已经是重要的. 并不是每一个人都赞同魏尔斯特拉斯对待基础问题的精确方法 (即通过级数、有理函数等). 说真的, 黎曼的更加几何化的方法, 不说是成了一个学派, 也吸引了许多追随者. 他的方法所提供的洞察力, 被人们热情地赞颂. 然而, 后世的讨论必须在这样一个水平上进行, 其严格性要能与魏尔斯特拉斯所达到的相媲美. 如果说对待分析基础的方法还会改变, 需要正是按照魏尔斯特拉斯那样来严格掌握极限的概念, 这一点是不会变的. 余下的还需要严格化的分析的主题, 就是数系的定义.

对于实数, 最成功的定义 (就后来的使用而言) 可能要算是戴德金[VI.50] 所提出的定义了. 戴德金和魏尔斯特拉斯一样, 以整数为基本, 然后把它们推广为有理数, 并且注意到它们所满足的代数性质正是现在所说的域[I.3 §2.2] 的性质 (域这个概念也应归功于戴德金). 然后他就来证明有理数满足一个所谓**三分律**. 就是说, 每一个有理数 x 把有理数集合分成三部分: 其一是 x 自身; 其二是大于 x 的一切有理数; 其三是小于 x 的有理数. 他也证明了大于或小于一个给定有理数的所有有理数都可以延伸到 (正或负) 无穷, 以及每一个有理数都对应于数直线上的不同点. 然而他还注意到, 在数直线上有无穷多个点并不相应于任意有理数. 利用数直线上每一点都应该对应于一个数这一思想, 他就利用**切割**来构造出连续统 (即实直线) 的其余部分. 所谓切割, 就是有理数的非空集合的有序对 (A_1, A_2), 其中第一个集合的每一个元都比第二个集合的每一个元小, 而合并起来又包含了所有有理数. 这种切割显然可以由一个有理数 x 来生成, 这时, x 本身或者是第一个集合的最大元, 或者是第二个集合的最小元. 但有时 A_1 既没有最大元, A_2 也没有最小元. 这时, 就用这个切割来定义一个新数, 它必然是无理数. 至此, 可以证明所有的切割都相应于实直线上的点, 所以再也没有被遗漏的了. 比较苛求的读者会觉得这是回避了问题, 因为数直线以某种方式构成连续统可能是一个隐藏的前提.

戴德金的构造对于什么是为实数找到基础的最好方法引起了大量的讨论, 特别

是在德国. 参加讨论的人中有康托、海涅 (Heinrich Eduard Heine, 1821–1881, 德国数学家, 不是诗人海涅), 还有逻辑学家弗雷格[VI.56]. 例如海涅和康托都把实数看成有理数序列的等价类, 并给出一种程序使得可以定义基本的算术运算. 法国数学家梅雷 (Hugues Charles Robert Méray, 1835 – 1911) 也提出一种非常类似的方法. 与此相对照的则有弗雷格, 他在《算术基础》(*Grundlagen der Arithmetik*) 一书中试图在逻辑的基础上建立整数. 虽然这种构造实数的方法并未结果, 但是他一直坚持, 各种构造都不应禁止考虑数学上的功能, 还应能够证明其中没有内在的矛盾, 他在这方面起了作用.

尽管在实数、无穷集合和分析的其他基本概念上已经有了大量的研究, 共识仍然是不可捉摸的. 例如有影响的柏林数学家克罗内克[VI.48] 就否认实数的存在, 而坚持认为所有真正的数学都必须放在有限集合的基础上. 他如魏尔斯特拉斯 (他们一同工作过, 而且克罗内克还对魏尔斯特拉斯有过影响) 一样, 强调整数和多项式之间有很强的类比, 并且企图用这个代数的基础来建立起整个数学. 所以, 对于克罗内克, 分析中的整个主要的研究道路都是一种诅咒, 他对此表示激烈的反对. 这些观点对于一些后来的作者, 直接或者间接地是有影响的, 其中就包括布劳威尔[VI.75] 和围绕着他的直觉主义学派, 还有代数学家和数论家亨泽尔 (Kurt Hensel, 1861–1941, 德国数学家).

所有为分析建立基础的工作都以这样或那样的方式, 基于深层的 (时常是未显示的) 量的概念之上. 然而, 从 1880 年代到 1910 年代这个时期, 分析的基础的框架移到集合理论上去了. 它起源于魏尔斯特拉斯的学生康托的工作, 康托在 1870 年代早期就开始研究傅里叶级数的不连续性. 于是康托就关心怎样区别不同类型的无穷集合. 他对于有理数和代数数都构成可数集合[III.11], 而实数集合则不可数的证明, 引导他到达不同基数的无穷集合的分层这个概念. 他的发现对于分析的重要性一开始并未得到广泛认可, 虽然早在 1880 年代, 米塔格–莱夫勒和赫尔维茨 (Adolf Hurwitz , 1859–1919, 德国数学家) 对于导集合 (即一个集合的极限点的集合) 以及稠密集或无处稠密集的概念, 都得到了值得注意的应用.

康托逐步达到了一个观点, 即集合可以起整个数学的基础的作用. 早在 1882 年, 他就写道, 集合的科学包含了算术、函数论和几何学, 而且以基数概念为基础, 给出一个 "更高级的统一". 然而这个提议表述得很含混, 因而开始时没有吸引到追随者. 然而, 集合还是设法进入了分析的语言, 最值得注意的是通过测度[III.55] 和集合的可测性的概念这条路. 事实上, 分析被集合理论吸收, 一条重要途径就是通过寻求哪些函数可以用来在抽象的意义下 "测度" 一个集合这条路走来的. 勒贝格[VI.72] 和波莱尔[VI.70] 在 1900 年左右关于积分和可测性的工作把集合理论以非常具体而亲密的方式捆绑到微积分上了.

建立分析的基础的下一个关键的一步是在 20 世纪初, 重新强调了对于数学理

论的公理结构. 这件事从希尔伯特得到了强有力的推动. 他从 1890 年代起就力求对几何学给出新的公理化. 佩亚诺[VI.62] 在意大利领导了一个学派, 具有类似的目标. 希尔伯特在这些公理的基础上重新定义了实数, 他的许多学生和同事, 由于这条道路所能提供的清晰性, 也热情地转向公理学 (axiomatics). 数学家不再去证明某些实体如实数的存在, 而是去安置一个系统使之满足实数所具有的基本性质. 实数 (或者什么别的对象) 就用所提供的公理来定义. 正如 Epple 所指出的那样, 这些实体被认为在本体论上是中立的, 就是说他们并未提出一种把实数区别于其他对象的方法, 甚至根本不提它们是否存在的问题 (Epple, 2003: 316), 集合论的问题以悖论的形式出现, 其中最著名的是罗素[VI.71] 的悖论: 设 S 是所有不包含自身的集合的集合, 则 S 不可能在 S 中, 也不可能不在 S 中. 策墨罗的公理学就力求避免这些困难, 部分地就是避免对集合下定义. 到了 1910 年, 外尔[VI.80] 就说数学是关于 "$\in$"(元素关系) 的科学, 而不是关于量的科学. 尽管如此, 策墨罗的公理学作为一种基本的战略, 仍然是有争议的. 至少有一点, 就是这个公理系统的相容性并未得到证明. 这样一种 "无含义" 的公理化, 就其把直觉完全排除在外, 也是有争议的.

在数学在 20 世纪初的复杂而迅速的发展背景下, 这些辩论在许多方面的意义已经远远超出了什么是分析中的严格性这一问题. 对于从事实实在在的工作的分析学家, 以及对于教授基本的微积分课程的教师, 这些问题对于日常的数学生活和教育, 至少是边缘的问题, 而我们正是这样对待它们的. 集合理论的语言已经渗透到用以描述基本对象的语言中了. 例如, 单变量的函数定义为有序的实数对的集合, 而有序对的集合论定义则是维纳[VI.85] 在 1914 年给出的, 函数的集合论定义也就是这个时候提出来的. 然而分析的研究与基础问题大不相同, 所以总想避免基础问题, 而且只要一个问题使用了基础方面的词汇, 一般人都会回避. 这绝不是说, 现代的数学家以完全形式的途径来对待分析. 与数和函数相关的直觉内容仍然是绝大多数数学家的思考的很大一部分. 关于实数和集合的公理只是构成一个框架, 以便在有需要时去引用, 但是基本的分析的本质的对象, 即导数、积分、级数及其存在和收敛的性态, 仍然是按照 20 世纪初期的办法来处理的, 所以关于无穷小和无穷的本体论的辩论就不那么活跃了.

鲁宾逊[VI.95](Abraham Robinson, 1918 –1974, 美国数学家) 对非标准分析的研究发表于 1961 年, 是这个故事的终曲. 鲁宾逊是模型论专家, 模型论研究的是逻辑的公理系统与可能满足它们的结构之间的关系. 他的微分是对正规的实数再加上 "微分" 的集合而得到的, 所得到的集合满足有序域的公理 (其中有实数所满足的算术), 但是此外还有小于一切 $1/n$(n 为任意正整数) 的元素. 在有些人看来, 这个创造消除了通常处理实数的许多不愉快的地方, 实现了莱布尼兹建立一个无穷小的理论的希望, 这个理论应该成为实数的同样结构的一部分. 鲁宾逊的工作虽然激起了

一阵活动, 从有些地方传来了相当大的喝彩, 但是鲁宾逊的方法从没有被广泛接受为分析的管用的基础.

进一步阅读的文献

Bottazini U. 1990. Geometrical rigor and "modern analysis": an introduction to Cauchy's Cours d'Analise. In *Cauchy* (1821). Bologna: Editrice CLUB.

Cauchy A L. 1821. *Cours d'Analyse de l'Ecole Royale Polytechnique: Première Partie—Analyse Algébrique.* Paris: L'Imprimerie Royale (Reprinted, 1990, by Editrice CLUB, Bologna).

Epple M. 2003. The end of the Science of Quantity: foundations of analysis, 1860-1910. In *A History of Analysis*, edited by Jahnke H N, 291-323. Providence, RI: American Mathematical Society.

Fraser C. 1987. Joseph Louis Lagrange's algebraic vision of the calculus. *Hietoria Mathematica*, 14:38-53.

Jahnke H N, ed. 2003. *A History of Analysis.* Providence. RI: American Mathematical Society/London Mathematical Society.

Riemann G F B. 1854. Ueber die Darstellbarkeit einer Funktion durch eine trigonometrische Reiche. *Königlichen Gesellschaft der Wissenschaften zu Göttingen*, 13:87-131. Republished in Riemann's collected works (1990): *Gesamelte Mathematische Werke und Wissenschaftliche Nachlass und Nachträge*, edited by R. Narasimhan , 3rd edn, 259-297. Berlin: Springer.

Weierstrass K. 1988. *Einleitung in die Theorie der Analytische Funktionen: Vorlesung Berlin* 1878, edited by Ullrich P. Braunschweig: Vieveg/DMV.

II.6 证明的概念的发展

Leo Corry

1. 引言和初步的考虑

在许多方面, 证明的概念的发展和数学整体的发展是共存的. 回顾过去, 人们可能首先以为数学是关于数、量、图形的科学知识的总体, 这些知识是由证明来论证, 而不是由实验和归纳推断来论证的. 然而, 这样的刻画不是没有问题的. 至少有一点, 这样刻画立刻就舍弃了人类文明史的重要篇章, 而那些篇章比起任意其他的智力活动, 更自然地是与数学相关的. 例如, 美索不达米亚文明和埃及文明都发展了很精细的知识的总体, 把它们描述成属于算术和几何学应该是最自然的了, 但是, 在其中找不到任何接近于后来数学中一般使用的那种证明的思想. 在几千块用楔形文字刻在泥板上的数学方法里, 如果说有什么论证的话, 那也是归纳的或者基

于经验的. 这些泥板上总是说, 遇到哪样的问题, 就使用哪种方法 —— 完全没有附加的解释, 也不打算给出一般的论证. 后来, 在中国、日本、玛雅或者印度文明中, 那些自然地与数学相关的领域也都有重要的发展. 这些文明寻求数学证明的思想的程度 —— 这是历史学家至今还在辩论的问题 —— 无疑不如希腊传统, 而且肯定不是采取典型的与希腊文明相联系的那种特定的形式. 虽然它们没有在某种一般的演绎的基础上得到论证, 难道我们不还是应该说, 这些也是数学知识的实例吗? 如果应该说还是, 那我们就不能再把数学刻画为得到证明支持的知识整体, 如前面做的那样. 然而, 这一张试纸肯定给出了一种有用的判据 —— 我们还不愿轻易地放弃 —— 借以把数学从其他智力活动里区别出来.

本文将集中讨论古代希腊的一个故事, 时间一般认为是始自公元前 5 世纪, 那时在希腊出现了一些独特的知识, 主要是关于数和图形的, 而其真理性可以并且要求以一种特殊的方法来论证 —— 具体说, 就是使用一种一般的演绎的论证, 即称为 "证明". 这个故事确切地始自何时以及如何开始并不清楚, 同样不清楚的是, 这样一种独特的思想的直接历史来源是什么. 因为在论证时强调逻辑和理由, 这种风俗和习惯远早于公元前 5 世纪在古希腊公共生活的其他领域 —— 如政治、修辞和法律 —— 里面已经根深蒂固, 所以数学证明的来源可能在那些领域里找到.

这个故事的早期阶段还存在一些其他问题, 既有历史方面的问题, 也有方法论方面的问题. 例如, 米利都的泰勒斯, 这是我们知道姓名的第一位数学家 (虽然他也是哲学家和科学家), 据说就**证明**过几个几何定理, 例如, 两相交直线所成的对顶角相等; 如果一个三角形的两个顶点位于圆的一条直径两端, 而第三个顶点又是圆周上另一点, 则此三角形必为直角三角形. 即令我们愿意按照其表面价值来接受这些传言, 也还是立即就有几个问题: 在何种意义下可以断定泰勒斯 "证明" 过这些结果? 更具体地说, 泰勒斯开始的假设是什么? 有哪些推断的方法他认为是有效的? 对于这些, 我们所知极少. 然而我们确实知道, 作为一个复杂的历史进程的结果, 最终发展出来一个知识体, 其中包括已知结果, 所使用的技术和问题 (既有已解决的, 也有未解决的). 这个整体逐渐也包括了经过调整的证明的思想, 即是以下的思想: 在所有情况下, 需要寻找的论证是某种一般的论证, 而不只是举一个例子 (甚至是举多个例子). 作为这个发展的一部分, 证明这个思想又与严格的演绎论证联系起来了, 而与例如对话式的论证 (就是讨论、协商) 和对真理作 "概然的推断" 相对立. 要想确定为什么出现的就是这种情况是一个有趣而又困难的问题, 我们在这里不讨论.

欧几里得[VI.2] 的《几何原本》是大约公元前 300 年编撰的. 它出类拔萃, 企图把基本概念、结果、证明和技巧组织起来, 以供想要掌握这个正在增长着的知识体的人之需. 在这一方面, 它是最成功最全面的尝试. 然而, 重要的是要强调指出, 在

希腊化的世界里,它并非唯一的尝试.这种努力并不只是一个把一些命题编撰起来,列为条文,并以之为经典这样的事情,在任何一个演进的学问中,在任何时候都可以找到这样的尝试.使数学与众不同的地方在于,它所包含的论断分成两类,而这种区分是至关重要的:一方面有基本的假设,或称*公理*,另一方面还有*定理*,定理典型地是更需精心阐述的命题,还必须说明它们是怎样由公理得出的——即是怎样证明的.在《几何原本》中是怎样想出这些证明,又怎样去实现它们,成了以后各个世纪的典范.

本文将要概要地讲解演绎证明的思想的演进.它最初在欧几里得式数学的框架中成形,后来,依次从古代希腊到伊斯兰世界,到文艺复兴的欧洲,到早期现代欧洲的科学,然后到 19 世纪和 20 世纪之初的主流数学,都实行这种演绎证明.本文主要的注意点放在几何学,其他领域如算术、代数则是在与几何学的联系中来处理的.这样的选择是由学科本身决定的.正如数学在科学中出类拔萃是由于只有它是依赖于证明的,欧几里得式的几何也是由此——最早是到 17 世纪——才在密切相关的学科中得到十分突出的地位.

其他学科里的结果,甚至整个学科,时常只是当已经提供了一个几何(或者几何式)的基础后才被认为是充分合法的.然而,19 世纪数学的重要发展,特别是与*非欧几何*[II.2 §§6-10] 以及*分析基础*[II.5] 相关,最终引导到了方向的基本转变,这时,算术(最终是*集合论*[IV.22])变成了确定性和清晰性的堡垒.而所有其他学科,包括几何学在内,都要从这个堡垒获得合法性和清晰性(见*数学基础中的危机*[II.7]).不过,甚至在这个基本转变之前,欧几里得式的证明已经不是孕育、发掘和实行数学证明的唯一途径了.本文既然主要关注几何学,就不能不舍弃一些后来成为合法的数学知识主流的重要发展了.在这方面,我们只举一个例子.一个在此不能探讨的基本问题是:数学归纳法的原理是怎样起源和发展及怎样被接受为一个普遍适用的合法的推理规则,而最终在 19 世纪后期被列为算术的基本公理之一的.此外,证明的概念的演化还涉及许多其他在此没有处理的方面,例如数学之分为各个子学科的内部组织的发展,还有数学与邻近学科的相互关系的变化.在另一个层次上,还与数学演化成一个有一定制度的社会事业有关.我们不来讨论证明是怎样生成的,怎样变成公众所接受的,怎样被传播、被批评、又时常被重写和改进的,这些都是有趣的问题.

2. 希腊数学

欧几里得的《几何原本》之所以是希腊数学的典范式著作,部分地是因为它所讲到的综合几何和算术的基本概念、工具、结果和问题,更加是由于它是如何对待数学证明的作用,以及这些证明应该取的形式.所有出现于《几何原本》里的证明

都由六个部分组成, 还加上附图①. 我们将以其中的命题 I.37 为例, 并且引用希思爵士的经典的译文, 但其中有些名词的含义与现在的用法稍有不同. 例如, 两个三角形“在相同平行线内”, 就是说它们的高相同而它们的底又位于同一直线上; 两个任意的图形“相等”, 就是说它们面积相等. 为了对读者作解释, 证明的各个部分的标题是本文作者加的, 原书是没有的. 说到附图就是指的图 1.

陈述 (protasis): 在同样的底上并在相同平行线内的两个三角形相等.

开始 (ekthesis, [现在译为“已知”]): 令 ABC, DBC 为在相同底边 BC 上的两个三角形, 并且位于相同的平行线 AD, BC 之间.

确定目标 (diorismos, [现在译为“求证”]): 三角形 ABC 等于三角形 DBC.

作图 (kataskeue): 在两个方向上延长 AD 到 E, F; 过 B 作 BE 平行于 CA, 在过 C 作 CF 平行于 BD.

证明 (apodeixis): 于是, 图形 $EBCA$, $DBFC$ 都是平行四边形; 它们是相等的, 因为它们是在相同的底边 BC 上, 而且在相同的平行线 BC, EF 内. 进一步, 三角形 ABC 是平行四边形 $EBCA$ 的一半, 因为直径 AB 平分此平行四边形; 而三角形 DBC 是平行四边形 $DBCF$ 的一半, 因为直径 DC 平分此平行四边形. 所以三角形 ABC 等于三角形 DBC.

结论 (sumoerasma): 所以, 在相同底边上并且位于相同的平行线内的三角形相等.

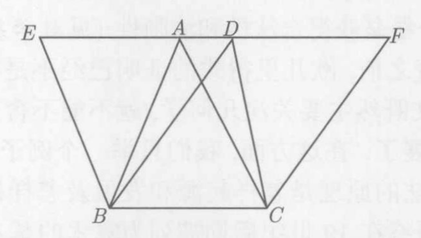


图 1　欧几里得《几何原本》的命题 I.37

这是一个关于图形性质的命题.《几何原本》里面还有一些关于需要完成的任务的命题, [即作图题]. 命题 I.1 就是一个例子: “在一有限直线上作一个等边三角形”. 这一类问题的解答同样也分成六个部分和附图. 在关于**算术**即数论的《几何原本》三卷里, 也是依照这个形式结构的, 最重要的是, 一定有附图. 举例来说, 考

①在 1940 年代以前, 我国有一些中学的初等几何教学也仿照此例, 要求学生证明几何题目也要分成几个部分并加附图. 这几个部分的标题, 我们按照希思的惯例, 对希腊文的说法不译, 而将希思的英文译文译为中文, 这些译文与希思的译文大体相同. 在前面说到的我国的教学方法中, 第一和最末两部分一般都不要求学生写出, 而第二部分差别较大, 通常把它写成“已知”或“假设”. 为方便读者, 我们在正文中对于有区别处都加以说明. 希思爵士 (Sir Thomas Little Heath, 1861–1940), 英国人, 是希腊数学经典著作的著名翻译家. —— 中译本注

虑命题IX.35, 其原来的版本如下:

如果任意多个数连续成比例, 而且从第二个数和最后一个数减去第一个数, 则第二个数之所余与第一个数之比, 和最后的数减去第一个数之所余与其前面所有的数的比相同.

冗长的文字第一次读起来可能很不好懂. 用比较现代的名词, 则一个与它等价的命题将是: 给出一个等比数列 $a_1, a_2, \cdots, a_{n+1}$, 有

$$(a_{n+1} - a_1) : (a_1 + a_2 + \cdots + a_n) = (a_2 - a_1 : a_1).$$

然而, 这样的翻译并没有传递原来的精神, 在原来的提法里面完全没有也不可能有任何的符号操作. 更重要的是, 现代的代数证明不能传递希腊的数学证明里附图无处不在, 甚至当并不需要一个真的几何作图时也是这样. 事实上, 命题IX.35 原来就有一个附图, 如图 2.

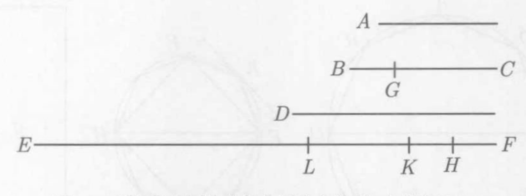


图 2 欧几里得《几何原本》的命题IX.35

它的证明的前几行如下:

设有任意多的数 A, BC, D, EF 从最小的 A 开始连续地成比例. 从 BC, EF 中各减去 BG, FH, 它们各等于 A. 则 GC 之于 A, 一如 EH 之于 $A, BC, D, \cdots$.

对于古代希腊在使用符号上的能力和局限, 这个命题及其证明是一个好例子, 特别是当他们并没有真正的符号语言时是怎样运作的好例子. 重要的是, 它们表明了哪怕是在理想的情况下, 希腊人也没有把证明看成是纯粹的逻辑构造, 而是看成一个用于图形的特别类型的论证方法. 图形并不只是对于论证的可视的帮手, 而是通过证明的**开始**或**已知**部分, 附图体现了由命题的一般特征和陈述所讲到的思想.

和附图在一起, 证明的六个部分在绝大部分的希腊数学里是典型的. 典型地出现在希腊数学里的作图和附图并不是随便作的, 而是今天我们所确认的圆规直尺作图. 在**证明**部分里的推理, 要么是直接的演绎推理, 要么是反证法, 但是结果总是事前就已知道的, 证明则是确认这种推理的手段. 此外, 希腊的几何思维, 特别是欧几里得式的几何证明, 都严格遵守齐次性定律 (见 [II.3 §5]), 即量只能和同一类的量 —— 数、长度、面积和体积相比较、相加、相减 (更详细的讨论, 可见数[II.1 §2]).

特别有趣的是, 那些关于曲线长度以及由曲线图形所包围的面积和体积的那些希腊证明. 希腊数学家没有能够表示多边形逐步逼近曲线以及最终趋向无穷的灵活的记号. 说真的, 他们设计了一种特殊类型的证明, 现在回头来看, 恰好就是隐含地涉及了趋向极限. 不过是在纯粹几何证明的框架下来做这件事, 因此照办无误, 遵从上面讲的六步的证明格式. 这种隐含的趋向极限, 基于使用一个连续性原理, 而后来这个原理又与阿基米德[VI.3] 联系起来了. 例如在欧几里得的陈述里, 这个连续性原理宣称: 给出两个不相等的同类的量 A 和 B(例如设它们都是长度、面积或体积), 而 A 大于 B, 如果从 A 中减去大于 $A/2$ 的量, 在从余下的量里再减去大于其一半的量, 把这个程序重复有限多次, 则最终会留下一个小于 B 的量. 欧几里得利用这个原理来证明例如两个圆的面积之比等于其半径的平方之比 (《几何原本》的命题 (XII.2)). 所用的方法, 即后来称为**穷竭法**的方法, 是基于所谓 **"双重反证"**, 成了以后好几个世纪的标准方法. 这个双重反证法可见图 3, 即这个命题的附图.

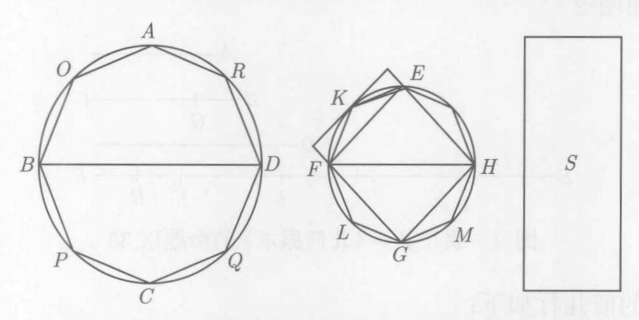


图 3 欧几里得《几何原本》命题XII.2 的附图

如果 BD 上的正方形与 FH 上的正方形的面积比不等于圆 $ABCD$ 与圆 $EFGH$ 的面积之比, 而等于圆 $ABCD$ 的面积与某个矩形 S 的面积之比, 这里 S 之面积或大于或小于圆 $EFGH$ 的面积. 用多边形来逼近这个曲边的图形, 因为连续性原理允许内接多边形的面积和圆的面积要多么接近就有多么接近 (比 S 与圆 $EFGH$ 的差别更加接近), 所以, 如果假设 S 小于或大于圆 $EFGH$ 就会达到 "双重矛盾".

在希腊的数学文献里, 有时也会找到除上述以外的证明和作图的形式. 其中包括基于两条直线上的同步运动的图形 [所作的曲线](例如多种三等分角线 (trisectrix), 如阿基米德螺线①)、多种机械装置 [所作的曲线] 以及以理想的机械 [(即力学)] 作为考虑的基础的推理. 然而, 只要可能, 上面所讲的欧几里得式的证明仍然是遵循的典范. 有一本 [后来发现的] 著名的阿基米德羊皮纸卷 (palimpsest) 提供了不甚经典的依据机械 (虽然是高度理想化的机械) 的思考方法, 用来给出关于面积

①三等分角线就是可以用来对任意角作三等分的曲线. 阿基米德螺线是其中一种, 它的极坐标方程是 $r = a\theta$.—— 中译本注

和体积的结果. 然而这也证实了理想的模式是优先的, 有一封阿基米德给埃拉托色尼 (Eratosthenes of Cyrene, 276 BC–194 BC, 希腊天文学家、数学家和地理学家) 的信, 他在信里展示了自己的机械方法的独创性, 但同时又尽量强调它只具有启发式的特性.

3. 伊斯兰世界的数学和文艺复兴时期的数学

正如欧几里得被看成是希腊数学的整个传统的代表一样, 阿尔 · 花拉子米[VI.5]也被看作是伊斯兰数学的代表. 他的工作始自 8 世纪后半叶. 从那时起直到 16 世纪出现了意大利的卡尔达诺[VI.7], 在这段时期里, 他的工作越来越变成数学发展的中心. 从其中与本文有关的部分来看, 他的工作有两个显著的特性: 一是"代数化"渗透到数学思想中去了, 二是为了使一般的数学知识的有效性合法化, 特别是使其中代数推理的有效性合法化, 他继续依赖欧几里得式的几何证明作为主要途径.

这两个特性结合的最好的例子可以在阿尔 · 花拉子米的开创性的著作《通过补全和还原作计算的纲要》(*al-Kitāb al-mukhatasar fī hisab al-jabr wa'l-muqābala*) 里面找到, 他在其中讨论了一些问题的解法, 其中未知的长度是与数和正方形 (其边长是一个未知数) 组合在一起的. 因为他只能看到正"系数"和正有理解有意义, 阿尔 · 花拉子米就需要考虑 6 种不同的情况, 每种情况下都需要用不同的方法来求出未知数, 发育完全的一般二次方程的思想, 以及适用于各种情况的求解的算法, 在伊斯兰的数学文献里是没有的. 例如"正方形和根等于数"这样的问题 (例如用现代记号写为 $x^2+10x=39$ 的方程) 以及"根和数等于正方形"这样的问题 (如 $3x+4=x^2$) 是看成完全不同的方程的, 其解法也就是不同的, 所以阿尔 · 花拉子米就把它们分开来处理. 然而, 在一切情况下, 阿尔 · 花拉子米都通过把它们翻译成几何语言, 然后依赖围绕着一个附图的欧几里得式的几何定理来证明他的解法的有效性. 值得注意的是这些问题中涉及的都是具体的数值的量, 他把这些数值的量与 [几何] 量连接起来, 又把这些几何量与附图联系起来. 这样, 阿尔 · 花拉子米就有趣地脱离了欧几里得式的证明风格. 希腊的齐次性定律基本上保留了下来, 因为通常在问题中涉及的三个量都是同类的, 即面积. 例如考虑方程 $x^2+10x=39$, 它就是阿尔 · 花拉子米的以下的问题:

什么是与 10 个根合并给出总数 39 的正方形? 求解的"方子", 规定为以下的步骤:

> 取根的一半 [5] 将它自乘 [25]. 把这个量加到 39 上得出 64. 取它的平方根 8, 从中减去根的一半, 余下 3. 所以数 3 就是这个正方形的一个根, 而正方形本身是 9.

图 4 给出了论证[①].

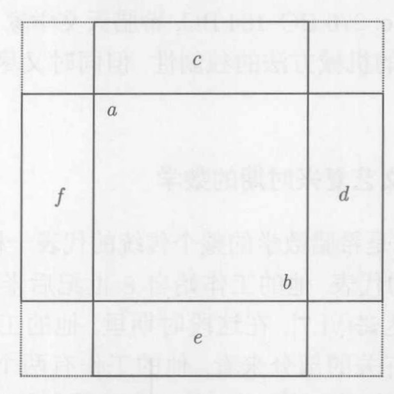


图 4 阿尔 · 花拉子米对于二次方程的公式的几何论证

[现在对图 4 作一些解释]. 图上的 ab 代表所说的正方形, 即 x^2, 而四个矩形 c, d, e, f 的面积各为 $\frac{10}{4}x$, 所以总和为题目中的 $10x$. [每一个矩形的短边应为 2.5], 所以图上的四个小正方形面积各为 6.25, [总和为 25. 用这四个小正方形把原图补全为一大正方形], 其面积为 64, 所以边长为 8. [减去两个小正方形的边长 5, 即得未知数解为 3].

年代比阿尔 · 花拉子米晚一代人的 Abu Kamil Shuja, 虽然解出了更多的问题, 也特别依赖于《几何原本》中的定理以及其附图来论证他的解法, 从而更加强了这个方法的力量. 欧几里得式的证明的优先地位已经为几何和算术所接受了, 现在又和代数方法结合, 最终变成了文艺复兴时代数学的主要主题. 卡尔达诺 1545 年写的《大术》(*Ars Magna*) 就是这个潮流的最早的例子, 其中给出了三次和四次方程式的完全的解法. 虽然他所采用和发展的代数思想路线变得更加抽象、更加形式化, 卡尔达诺仍然参照基于附图的欧几里得式的几何论证作为自己的论据和解法的根据.

4. 17 世纪的数学

证明的概念的下一个显著的改变出现在 17 世纪. 数学在这个时期的最有影响的发展是牛顿[VI.14] 和莱布尼兹[VI.15] 同时创立的无穷小计算. 这个重大的发展是几乎跨越了整个世纪的过程的顶点, 涉及引入和逐渐改进重要的技巧来求出面积和体积、切线的梯度以及极大和极小. 这些发展既包括了可以追溯到希腊经典著作

①图 16 的要点从几何上看很清楚, 就是把一个图形 “补全” 成为一个正方形, 也就是我们说的 “配方法”. 阿尔 · 花拉子米原书名英译为 *The Compendious Book on Calculation by Completion and Balancing*, completion(完全) 之意应是 “补全”, 而 balancing(平衡) 前面已经指出就是现在我们说的 “移项”. 说是 “还原” 理由很清楚. 此处的中文译文就是这样拟定的 —— 中译本注

中的传统观点的详尽展开, 也包括了引进全新的概念如“不可分量”. 对于“不可分量”作为数学证明的合法工具的地位有过激烈的辩论. 同时, 由文艺复兴时代数学家和追随他们的伊斯兰先行者继续扩展代数技巧和途径, 现在得到了更大的推动力而逐步融入——由费马[VI.12] 和笛卡儿[VI.11] 带头——可以用于证明几何结果的工具的武器库. 在这些不同的潮流下面, 有着数学证明的不同的概念和实践. 下面来作一个简短介绍.

在费马的工作里可以看到, 经典的希腊几何证明的概念是如何本质上得到遵守而同时又富有成果地得到修正和扩展的例子, 这可以从费马计算广义双曲线 (用现代记号来写就是 $(y/a)^m = (x/b)^n, m, n \neq 1$) 及其渐近线所包围的面积看到.

例如, 二次双曲线 (即由 $y = 1/x^2$ 所表示的曲线) 在这里是由其上任意两点的纯粹几何关系来定义的, 具体说这两点的横坐标上的正方形面积之比与它们的纵坐标成反比: $AG^2 : AH^2 :: IH : EG$(见图 5). 应该注意, 这并不是按照现代的字面意义下的一个方程式, 在方程式上面是可以直接完成标准的符号操作的. 这是一个可以应用希腊数学的经典规则的四项比例式. 证明也是完全的几何证明, 而且本质地是按照欧几里得式的风格的. 这样, 如果按照连续的比例 [即按几何序列取横坐标] 来取线段 AG, AH, AO 等等, 则可以证明矩形 EH, IO, NM 等等也成连续比例, 即 $EH : IO :: IO : NM :: \cdots :: AH : AG$.

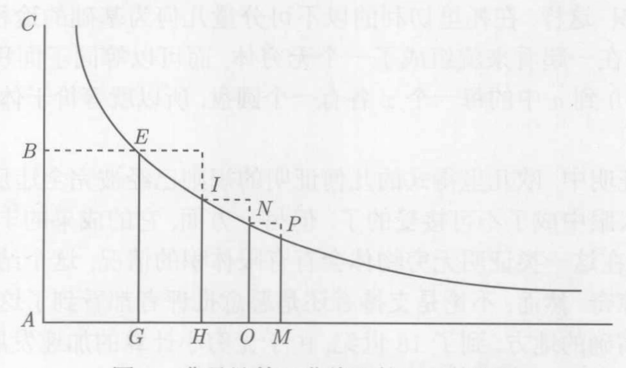


图 5 费马计算双曲线下的面积的附图

费马在这里应用了《几何原本》中的命题IX.35(这个命题在前面提过). 这个命题中包含了几何数列中任意多个量的和, 具体说来 (用现代记号就是),

$$(a_{n+1} - a_1) : (a_1 + a_2 + \cdots + a_n) = (a_2 - a_1) : a_1.$$

但是就在这一个关节点, 他的证明发生了一个有趣的改变, 他引入了一个有点晦涩的概念 “adequare”, 这个词他是从丢番图的著作里找到的, 就是许可作 “近似地相等”. 具体地说, 正是这个思想帮助他回避了在希腊几何里典型地使用的双重反证

方法, 也就是一种隐含的趋向无穷. 一个由 GE 和水平渐近线以及双曲线所包围的图形 [面积] 等于这样一些矩形 [的面积] 的无穷和, 这些矩形是当矩形 EH“消逝而化为乌有”时得出来的. 此外, 命题IX.35 蕴含着此面积等于矩形 BG. 值得注意的是, 费马在此仍然选择依赖于古人的权威, 当他宣布这个结果时, 仍然暗示着双重反证方法. 他说:“很容易用比较长的按阿基米德的方式 [的证明] 来验证它”.

这种把已经被接受的几何证明的经典 [的应用范围] 加以扩展的企图, 最后引导到了更加进取的与不可分量相关的途径. 这种途径是卡瓦列里 (Bonaventua Francesco Cavalieri, 1598–1647, 意大利数学家)、罗伯瓦尔 (Gilles Personne Roberval, 1602–1675, 法国数学家) 和托里切利 (Evangelista Torricelli, 1608–1647, 意大利数学家) 所使用的. 托里切利计算一个无穷物体的体积的例子很好地说明了这个途径, 这个物体就是 (用现代语言来说) 将双曲线 $xy = k^2$ 的 x 之值从 0 到 a 的一段绕 y 周旋转而成的旋转体.

不可分量的基本思想是把面积看成无穷多个直线段的总和或者说集合, 体积则看成无穷多个面积的总和或者集合. 托里切利在计算这个旋转体的例子时, 就把它看成无穷多个边界曲面为弯曲的柱面的总和, 这些柱面一个套着一个, 其半径则从 0 变到 a. 用现代代数用语, 则半径为 x 的柱面高为 k^2/x, 所以它的弯曲表面的面积是 $2\pi x\left(k^2/x\right) = \pi\left(\sqrt{2}k\right)^2$, 这是一个与 x 无关的常数, 而等于一个半径为 $\sqrt{2}k$ 的圆的面积. 这样, 在托里切利的以不可分量几何为基础的途径下, 所有这些柱面的集合, 放在一起看来就组成了一个无穷体, 而可以等同于面积为 $2\pi k^2$ 的圆盘的总和, 对于 0 到 a 中的每一个 x 各有一个圆盘, 所以就等价于体积为 $2\pi k^2 a$ 的圆柱.

在这一类证明中, 欧几里得式的几何证明的规则已经被完全违反了, 这就使这些证明在许多人眼中成了不可接受的了. 但另一方面, 它的成果的丰硕又使它很有吸引力, 特别是在这一类证明无穷物体会有有限体积的情况, 这个结果甚至使得托里切利也大感惊奇. 然而, 不论是支持者还是恶意批评者都看到了这一类技术可能引起矛盾和不精确的地方. 到了 18 世纪, 由于无穷小计算的加速发展, 与之相关的技术和概念与不可分量相关的技术基本上都消失了.

欧几里得式的几何证明所确立的界限在另一方向上也被跨越了, 这就是在笛卡儿手上的包罗一切的几何的代数化. 笛卡儿采取的基本步骤是引入单位线段作为用于几何证明的图形的关键元素. 这一步骤所蕴含的根本性的创新在于允许对于线段进行种种运算, 而这是迄今没有可能做到的. 这一点笛卡儿在他的《几何》(*La Géométrie*) 一书中强调如下①:

算术仅由四种或五种运算组成, 即加、减、乘、除和开方根, 后者可以认为是

①以下的译文借用了此书中译本 (袁向东译, 武汉出版社, 1992 年出版) 第 3 页, 但稍有修改. —— 中译本注

一种除法; 在几何中, 为得到所要求的直线段, 只需对其他一些线段加加减减; 不然的话, 可以取一个线段, 称之为单位, 目的是把它同数尽可能紧密地联系起来, 而它的选择一般是任意的; 当再给定其他两条线段, 则可求第四条线段, 使它与给定直段之一的比等于另一给定线段与单位线段之比 (这跟乘法一致); 或者, 可求第四条直线段, 使它与给定线段之一的比等于单位线段与另一线段之比 (这等价于除法); 最后, 可在单位线段和另一线段之间, 求一个、两个或多个比例中项 (这相当于求给定直线的平方根、立方根, 等等).

这样, 例如给出图 6 的两个线段 BD, BE, 则 BC 就表示 BE 除以 BD 的商. 图中的 AB 就是单位长.

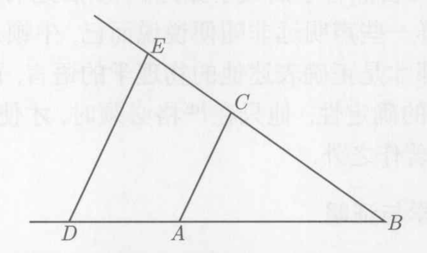


图 6 两个已给线段的除法的笛卡儿几何计算

从表面上看这个证明是欧几里得式的几何证明 (因为这里有附图, 并且应用了相似三角形), 但是引进单位长度, 并且用它来定义一种运算, 就使它与欧几里得式的几何证明从根本上分道扬镳了, 而且为几何证明打开了完全的新天地. 这不仅是因为迄今在欧几里得式的证明里面从来没有出现过长度的量度, 还由于这些运算存在, 传统上与几何定理联系在一起的必不可少的维度失去了意义. 笛卡儿使用了 $a-b, a/b, a^2, b^3$ 还有它们的根式这些表达式, 但是他强调, 这些表达式只应该 "简单地理解为一些线段, 只不过我使用了代数里用的名词, 如平方、立方等等." 由于消除了维度, 齐次性也就不必要了. 笛卡儿和他的前人不同, 前人只是当量有直接的几何意义时才能掌握量, 笛卡儿在形成 a^2b^2-b 并求其立方根时就不感到有任何问题. 为了这样做, 他说 "我们必须认为 a^2b^2 已经被单位除过一次, 量 b 则已被单位乘了两次" [(从而都与立方有相同维度)]. 这些话希腊几何学家和他们的伊斯兰以及文艺复兴的追随者根本不可能理解.

几何学的代数化, 特别是可以用代数程序来证明几何事实这样一个新的可能性, 是与以下的事实强烈地相关的, 这就是当时把代数式子看成自立的数学实体, 对于它们有着众所周知的形式操作规则, 可以系统地应用, 这样一种思想已经很巩固了. 这个思想直到 1591 年左右, 才在维特[VI.9] 手上完全成熟. 但是并非 17 世纪所有的数学家都看到了与代数思想相关的重要进展, 既没有把它看成是应该自然的

接纳的方向, 也没有把它看成是代数这一分支的进步的清楚的信号. 一个著名的反对任何偏离几何学中古典的欧几里得式的途径的人不是别人, 就是牛顿[VI.14], 他在《万有算术》(*Arithmetica Universsalis*)(1707 年) 一书里很肯定地表达了自己的观点:

> 方程式是算术计算的表达式, 适当地说, 在几何学中没有地位, 除非是利用它们来证明真正的几何量 (直线、曲面、立体和比例) 彼此相等. 乘法、除法和这一类计算近年来被引入了几何学, 轻率而且违反了科学的最初的原理……所以, 这两门科学不应该搞混, 而最近几代人, 因为把它们搞混了, 已经失去了简单性, 而几何学的全部优雅尽在于此.

牛顿的《原理》[(即《自然哲学的数学原理》, 以后此书一律这样简称)] 证实了这样一个事实, 就是这样一些声明远非随便说说而已, 牛顿是前后一贯地偏爱欧几里得风格的证明, 认为那才是正确表述他的物理学的语言, 而正是这种语言赋予了这种物理学以最高程度的确定性. 他只在严格必须时, 才使用自己的微积分, 而把代数完全排除在自己的著作之外.

5. 18 世纪数学的几何学与证明

数学分析成了 18 世纪数学家的首要的注意焦点. 自微积分开始发展以来, 关于分析基础的问题就产生了, 一直到 19 世纪晚期才尘埃落定. 这些问题在相当大的程度上都涉及合法的数学证明的本质. 长期以来几何学作为数学的确定性的基础地位是无争议的, 现在, 关于分析基础的辩论, 在破坏这种地位上起了重要作用, 而这种基础的地位, 现在被赋予了算术. 这个过程的第一个重要的阶段, 是欧拉[VI.19]对于微积分的重新陈述. 微积分一旦从它的纯粹几何的根源分离开来, 就以代数指向的函数概念为中心. 这种置代数于几何之上的潮流, 在欧拉的继承人那里得到了进一步的推动. 例如, 达朗贝尔[VI.20] 就把数学的确定性超乎其他地与代数相联系 —— 因为代数有更高的一般性和抽象性 —— 然后才是几何与力学. 这一点清楚地离开了牛顿和他的同时代人的观点. 在拉格朗日[VI.22] 手上, 这个趋势达到了高峰而且成了经过仔细构思的纲领, 他在自己 1788 年的《解析力学》(*Méchanique Analytique*) 一书的序言里表达了一种激进的观点, 对于怎样才能达到数学科学的确定性, 并与几何学保持距离, 他说过一段非常著名的话:

> 在本书里, 找不到图形, 我所详细解释的方法, 既不需要作图, 也不需要几何和力学的论证, 而只需要代数运算, 服从于一个正规的均匀的进程.

这些发展的细节不在本文的范围之内. 然而重要的是要强调, 尽管有这样一些相当大的冲击, 在更加属于主流的**几何学**这个领域里, 证明的基本概念在 18 世纪里变化并不很大. 那个时代的哲学家, 特别是康德, 对于这些概念提出了很有阐明力量的展望.

康德对于那个时代的科学, 特别是数学, 有很深刻的知识. 他对于数学知识和证明的**哲学讨论**, 本不是本文关心的事. 但是既已知道了他对于那个时代的观念都很熟悉, 则康德的观念对于当时对证明的理解, 还是提供了一个具有洞察力的**历史展望**. 特别有兴趣的是, 他对于一方面的哲学论据和另一方面的几何证明作了什么样的对比? 前者关心的是一般的观念, 后者则是求助于 "视觉的直觉"(就是康德意义下的直觉, 德文为 Anschauung) 研究具体的然而是非经验的观念. 这个区别被概括在他的《纯粹理性批判》里面的一段很有名的话里:

> 设把一个三角形的概念给了哲学家, 让他以自己的方式去找出三角形的内角和与直角的关系. 他除了有三条直线围成的有三个角的图形这个观念以外, 什么都没有. 不论他对这个观念沉思多久, 他也永远不会产生出任何新东西. 他可以分析或澄清直线或者角或者这个数的观念, 但是他永远得不出尚未包含于这些观念之内的东西. 现在让几何学家来对待这个问题, 他会马上就作出一个三角形来. 因为他知道两直角之和恰好等于两个相邻的角之和, 这两相邻的角是他在直线上取一点作出来的, 于是他把他的三角形的一边延长而得到两个相邻角, 它们加起来等于两直角. 然后他用平行于对边的平行线把外角分开, 而且看到有一个相邻的外角等于一个内角, 如此等等. 用这种方式通过一个自始至终由直觉引导的推断的链条, 他得到了问题的充分明显而且普遍有效的解答.

简而言之, 对于康德, 数学证明的实质使它区别于其他种类的演绎论证 (如哲学) 之处就在于图形的中心地位和所起的作用. 正如在《几何原本》中, 图形并不是对于无非是抽象推理的启发性的帮助, 而是一种 "直觉", 是数学思想的一个奇异的体现, 这个思想不仅存在于空间里, 而且存在于空间和时间里. 事实上,

> 我无法不在自己的思想里画一条直线, 不论多么小, 用来表现出一条直线, 在思想里面, 直线是从一个点开始逐渐生成的. 只能这样获得直觉.

正是图形作为 "可视的直觉" 所起的作用为康德提供了一种解释, 说明为什么几何学不是一门经验科学, 也不是没有任何综合内涵的巨大的重言式. 按照他的观点, 几何证明受到逻辑的制约, 但远远不只是对于所用的名词的逻辑分析. 这个观点是一种新颖的哲学分析的核心, 它的起点正是关于什么是数学证明的当时已经根深蒂固的观念.

6. 19 世纪的数学和关于证明的形式观念

19 世纪在几何学和数学的各个分支里都充满了重要的发展, 不仅是在其方法上, 它们的目的也有了变化. 作为一个知识领域, 逻辑也经历了显著的变化, 逐步的数学化完全改变了它的领域和方法. 所以, 到了 19 世纪末, 证明的概念及其在数学中的作用都有了深刻的变化. 1854 年, 黎曼[VI.49] 在哥廷根作了具有首创意义的

演说: "**论作为几何基础的假设**". 大约同时, 波尔约 [VI.34] 和罗巴切夫斯基[VI.31] 在非欧几何上的工作, 以及高斯[VI.26] 的有关思想, 论时间始于 1830 年代开始为公众所知晓. 一种相容的但是不相同的几何学的存在, 迫切地需要重新修正关于几何知识的本质的最基本的长期存在的信念, 其中当然也包括证明和数学严格性的作用. 这方面更值得注意的是对于射影几何学[I.3 §6.7] 的兴趣的重新兴起. 在彭赛列 (Jean-Victor Poncelet, 1788 –1867, 法国数学家) 的著作 [《论图形的射影性质》(*Traité des propriétés projectives des figures*)] 在 1822 年出版以后, 射影几何学又变成了一个很活跃的研究领域, 有自己的未解决的研究课题以及基础问题. 射影几何学加到了许多别的几何学的展望之中, 更是促进了一种 [把各种几何学] 统一起来并加以分类的努力, 其中最有意义的是那些以群论为基础的思想, 尤其是克莱因[VI.57] 和李[VI.53] 在 1870 年代的著作最值得注意. 1882 年, 帕施 (Moritz Pasch, 1843–1930, 德国数学家) 发表了一部有影响的关于射影几何学的著作: [《新几何学讲义》(*Vorlesungen über neuere Geometrie*)], 致力于系统地探讨射影几何学的公理基础和基本定理的相互关系. 帕施的书也试图把多年来所发现的欧几里得几何的逻辑漏洞填补起来. 他比 19 世纪同时代的所有数学家都更系统地强调, 几何学的所有结果都应该从公理开始, 经由严格的逻辑演绎得出, 而不应依赖于解析的手段, 特别是不应求助于图形以及所涉及的图形的性质. 这样, 虽然他是以某种方式回归到欧几里得式证明的法典 (到那时已经有所放松), 但是他对于图形的态度 [却与欧几里得式的证明] 基本不同. 由于认识到可视的图形潜在的局限性 (以及可能有误导的影响). 帕施比起他的前人更加强调证明的纯粹逻辑结构. 尽管如此, 帕施还没有走到对于几何学的完全形式主义的观点. 他对于几何学的起源和意义, 一贯地还是采取了一种经验主义的途径, 还达不到公然宣布图形只有启发作用的地步. 他说:

> 几何学的基本命题, 没有相应的图形是无法理解的, 图形表示的是从某些确定的简单的事实所观察到的东西. 说定理不是观察出来的, 而是证明出来的更为恰当. 在演绎中所完成的每一项推断都必须要在图形中确认一下, 但是它并非由图形来论证, 而只能用以前的某个命题 (或定义) 来论证.

对于图形在几何证明中失去中心地位, 而让位于纯粹的演绎关系, 帕施的工作肯定是有贡献的, 但是他的工作还没有直接引导到对于公理在几何学中的地位做彻底的重估, 也还没有改变以下的观念, 即几何学研究的基本上是空间的视觉的直觉 (即 Anschauung). 19 世纪几何学最重要的发展, 在多个因素的联合作用下, 才在证明的观念上产生出显著的变化. 数学分析仍然是第一位的研究领域, 对它的基础的研究必然越来越强烈地成为对算术的严格性的研究, 而不再是对几何的严格性的研究. 这个转变是受到诸如柯西[VI.29]、魏尔斯特拉斯[VI.44]、康托[VI.54]、戴德金[VI.50] 这样一些数学家的工作的驱使, 这些工作的目标是消除直觉的论证和概念, 代之以越来越基本的命题和定义 (事实上, 一直到 20 世纪的最后的三分之一,

在戴德金关于算术的基础的工作中，这些工作所追求的严格陈述才得到了公理的支持). 研究数学理论的公理基础，不论是几何、代数还是算术，以及探寻另外的可能的公设系统，这样的思想在整个 19 世纪一直有数学家们在追求，这些人中有皮科克 (George Peacock , 1791–1858, 英国数学家)、巴贝奇 (Charles Babbage, 1791–1871, 英国数学家)、赫什尔爵士 (Sir John Herschel, 1792–1871, 英国数学家和天文学家, 他的父亲 William Herschel 以发现天王星而著名), 还有在地理和数学背景上都不相同的格拉斯曼 (Hermann Günther Grassmann, 1809–1877, 德国数学家). 但是这些研究在当时只是例外，而非常规，而在形成分析和几何中的证明的新观念上作用有限.

把以上这些潮流汇合起来形成关于证明的概念的新研究途径的一个主要转折点的是意大利的*佩亚诺*[VI.62] 和他的追随者的工作. 佩亚诺的主流的活动表明他是一位能干的分析学家，但是他又对人造的语言有兴趣，特别是对发展一种人造语言来对数学证明完全形式化这件事有兴趣. 1899 年，他在算术中应用这种概念中的语言的完全成功，给出了他的著名的*自然数的公设*[VI.67]. 帕施关于射影几何的公理系统的工作是对佩亚诺的人造语言的一项挑战. 于是他就着手来研究在几何学的演绎结构中涉及的逻辑名词与几何名词之间的关系. 在这个背景下，他提出了独立的公理之集合的概念，并且把这个概念用于他自己的射影几何公理系统，这与帕施的系统稍有区别. 这个观点并没有把佩亚诺引导到关于证明的完全的形式主义观点，他仍然在非常相似于他的前人的词语下来构思几何学:

> *谁都可以提出假设，并且发展其逻辑后果. 然而，如果谁想把这个工作冠以几何学之名，这些假设或公设就必须能够表示对于物理图形所作的简单而初等的观察的结果.*

在佩亚诺的影响下，皮耶里 (Mario Pieri, 1860–1913, 意大利数学家) 发展了一种符号系统来掌握抽象形式理论. 皮耶里和佩亚诺与帕施不同，他前后一贯地在推进这样一个观点，即把几何看成纯粹逻辑系统，而定理则由假设的前提导出，而且基本的名词都没有任何经验的或直觉的意义.

19 世纪最后一年，出版了希尔伯特的《几何基础》(*Grundlagen der Geometrie*, 1899) 一书[①]，打开了几何学和几何证明历史的新篇章. 这本书综合了前面所说的几何研究的各种潮流，并使它们完备. 在这部著作中，希尔伯特能够对射影几何的基本结果，如德萨格 (Girard Desargues, 1591–1661, 法国数学家) 定理和帕普斯 (Pappus of Alexandria , 约公元 290 – 350 年，古希腊的最后一位伟大几何学家) 定理的逻辑关系作全面的分析，而且特别注意到连续性的考虑在这些证明中的作用. 他的分析

①此书后来有多个版本，而且历经补充与修订. 早在 1924 年，傅种孙教授就根据英文第一版把它翻译为中文. 1958 年，又由江泽涵教授将其第七版从俄文译本转译为中文. 1992 年由朱鼎勋教授根据最新的第十二版对江译本再增补与修订，由科学出版社分上下两册重新出版. —— 中译本注

是基于引入一种广义的解析几何, 其中的坐标可以取自不同的数域[III.63], 而不仅是实数. 这样一个途径就对任意一种给定的几何学创造了一个纯综合的算术化, 这样也就澄清了欧几里得几何学作为一个演绎系统的逻辑结构. 这部书也澄清了欧几里得几何和各种已知的几何学 —— 非欧几何、射影几何和非阿基米德几何的关系. 这种对于逻辑的专注, 意味着图形被贬为仅具有启发的作用. 事实上, 虽然在《几何基础》的很多证明里仍然有附图, 但是逻辑分析的整个目的就在于避免为图形所误导. 证明, 特别是几何证明, 就这样变成了纯粹的逻辑论证, 而不是对于图形的论证. 同时, 作为相关问题推导的出发点的公理, 其本质和作用也有了变化.

希尔伯特在帕施带领之下, 引入了几何学的新的公理系统, 目的在于填补先前的系统遗留下来的逻辑空隙. 这些公理分成五组 —— 关联公理、顺序公理、合同公理、平行公理以及连续公理, 每一组公理都表示了空间直觉在我们的理解中的特殊的展现方式. 公理是对三种基本类型的对象提出的: 点、直线、平面. 这些对象则是无定义的, 而公理就意味着为它们提供了隐定义. 换句话说, 不是先定义点、直线和平面, 然后给出它们应该满足的公理, 而是不去定义它们, 只说它们是一些满足所设定的公理系统的实体. 此外, 希尔伯特要求, 一个系统里的各个公理应该是互相独立的, 而且引进了一种方法来检验这个要求是否得到满足. 为此, 他建立了一种新几何学的模型, 使这个新几何学只是不满足系统中的某一个给定的公理, 但满足其他公理. 希尔伯特也要求这些规律是相容的, 而在他的公理系统中, 这种相容性又被证明为依赖于算术的相容性. 一开始, 他以为证明算术的相容性并不是大的障碍, 很久以后才发现情况并非如此. 希尔伯特在一开始还对公理系统提出了两个附加的要求: 简单性和完全性. 所谓简单性, 基本上就是要求一个公理不包含多于 “单一的” 一个概念. 然而, 系统中的各个公理都应该是 “简单的” 这一要求, 在希尔伯特和他的后继者的工作里, 都从未清楚地定义过, 也没有系统地追求过. 最后一个要求, 即完全性, 希尔伯特在 1900 年对其的理解是: 一个数学领域的充分的公理化, 应该允许导出这个领域的**所有**已知的定理. 希尔伯特宣称, 他的公理确实能够给出欧几里得几何的所有已知的结果. 但是他不能形式地证明这一点. 事实上, 因为对于任意已给的公理系统, “完全性” 这个性质都不可能形式地加以核验, 所以, 完全性就没有成为对于公理系统的标准要求. 重要的是要注意, 1900 年希尔伯特所使用的完全性概念, 和现在被接受的模型论的完全性概念完全不同. 后者出现得晚得多, 相当于要求在一个公理系统中, 每一个真命题, 不论是已知还是未知, 都应该是可证明的.

应用无定义元素以及随之而来的公理作为隐定义这个概念, 对于把几何看作如皮耶里所设计的逻辑系统起了重大的推动作用, 而且最终改变了什么是数学的真理性, 什么是数学证明的观念. 希尔伯特在不同的场合宣布过 —— 这是戴德金的思想的回声 —— 在他的系统里, “点、直线、平面” 这些词可以换成 “椅子、桌子、啤

酒杯”, 而在任何意义下都不影响理论的逻辑结构. 此外, 按照希尔伯特在关于集合论的悖论的讨论, 他强力地强调: 由公理来隐定义的概念的逻辑相容性, 正是数学存在性的本质. 在这些观点的影响下, 由于希尔伯特引入的新方法论工具的影响, 以及由此得到的对于几何基础的成功的概述, 许多数学家继续推进关于数学的新观点, 而许多新的数学活动也在这种或那种意义下超过了体现在希尔伯特的途径中的观点. 另一方面, 在 20 世纪初, 在美国繁荣起来的由 E.H. 摩尔 (Eliakim Hastings Moore, 1862 –1932, 美国数学家) 领导的一个潮流, 把对于公设系统的研究本身变成了一个自身有意义的数学领域, 而与这个系统所定义的领域的研究无关. 例如, 这些数学家定义了群、域、射影几何等学科的独立的公设系统的最小集合, 而不继续研究群、域、射影几何这些个别的学科. 另一方面, 许多著名的数学家开始接受和发展关于数学真理和数学证明的更加形式主义的观点, 并且把它们用到越来越多的数学领域里去. 激进的现代主义数学家*豪斯道夫*[VI.68] 的工作就是这个潮流的重要例子, 他是一贯地把希尔伯特的成就与对于几何学的形式主义观点联系起来的第一批数学家之一. 例如, 在 1904 年他就写道:

> 自康德以来的哲学辩论中, 数学, 至少是几何学, 总是被看成受制于其他因素, 即依赖于外来的因素, 这种因素没有更好的名称, 我们也就称之为直觉, 可能是纯粹的或经验的, 可能是主观的或经过科学改进的, 可能是内生的或后天获得的. 现代数学最重要的也是最基本的任务, 一直是使它从这种依赖性下解放出来, 奋斗出一条从受治到自治的道路.

在 1918 年左右, 希尔伯特也追随过这样一种观点, 那时, 他正置身于关于算术的相容性的辩论, 并且提出他的 “有穷论” 的纲领. 这个纲领确实采取了强烈的形式主义观点, 但是他这样做, 却只有一个有限制的目的, 就是要解决算术的相容性这个特定的问题. 重要的是要强调, 希尔伯特关于几何的观念, 过去是, 现在仍然是, 本质上经验主义的, 他从来没有把对于几何学的公理化分析看成一种对于数学的整体的形式主义观念. 他是把公理化的途径看成是一种对现存的很精巧的理论的进行概念的澄清的工具, 而几何学只是提供了这些理论的一个最卓越的例子.

希尔伯特关于证明的概念的公理化途径, 对于数学中的证明和真理性的隐含的意义, 在一些数学家里引起了强烈的反响, 最著称的当推来自*弗雷格*[VI.56] 的反响. 弗雷格的观点与逻辑学的地位在 19 世纪和 20 世纪之交的变化与逻辑学的逐渐数学化、形式化有关. 这个过程是 19 世纪许多数学家不断努力的结果, 这些数学家有*布尔*[VI.43]、*德 · 摩根*[VI.38]、格拉斯曼、皮尔斯 (Charles Sanders Peirce, 1839–1914, 美国哲学家、逻辑学家)、施洛德 (Friedrich Wilhelm Karl Ernst Schröder, 1841–1902, 德国数学家和逻辑学家), 他们的工作是指向于把逻辑代数化. 然而, 逻辑学向一种新的形式的概念前进的最有意义的一步, 是对于*逻辑量词* [I.2 §3.2](全称量词 $\forall$ 和存在量词 $\exists$) 在形成现代的数学证明中的作用的进一步了解. 在分析的严格化以及

远离视觉直觉的过程中, 这种了解以一种非形式的然而日渐清晰的时尚而出现, 并且是这个过程的一部分, 特别是在柯西、波尔扎诺[VI.28] 和魏尔斯特拉斯的手上. 量词第一次被形式化地定义, 并且系统地列为条文, 是弗雷格在他 1879 年所写的《概念手稿》(*Begriffschrift*) 一书中. 弗雷格的系统以及稍后由佩亚诺和罗素[VI.71] 提出的类似系统, 把量词和命题连词的区别, 以及逻辑符号与代数或算术符号的区别, 清楚地放在我们面前.

弗雷格提出了**形式系统**的概念, 在其中, 所有许可的符号、所有产出适当定义的公式的规则、所有的公理 (即预先选定的适当定义的公式), 还有所有的推理规则, 都要事先给出. 在这样的系统里, 所有的演绎都可以按照**句法**来检验 —— 换句话说, 都可以用纯粹的形式的手段来检验. 在这种系统的基础上, 弗雷格的目的是要生产出其证明没有逻辑漏洞的理论. 这不仅适用于分析及其算术基础 —— 正是这些领域为弗雷格提出了其工作的动机, 还要适用于随时间演进的几何学的新系统. 另一方面, 在弗雷格看来, 数学理论的公理 —— 虽然它们只是作为适当定义的公式出现在形式系统中 —— 却体现了世界的真理. 这就是他对希尔伯特的批评的基础. 弗雷格断言, 是公理的真理性确定了它们的相容性, 而不是如希尔伯特相反地确定的, 是公理的相容性决定了它们的真理性.

我们这就看见了两个分离的领域 —— 几何学和分析 —— 的基础研究, 其灵感来自不同的方法论和不同的哲学观点, 却在 19 世纪和 20 世纪之交汇合在一起, 创造了对于数学证明的全新的观念. 按照这个观念, 数学证明被看成纯粹的逻辑结构, 在纯粹句法的意义下适用, 而与来自图形的视觉直觉无关. 自那以后, 这个观念统治了数学.

结束语: 20 世纪的证明

到了 20 世纪初, 证明的概念已经稳定下来, 成为什么才是有效的数学证明的理想模型, 这一点至今还为人们广泛接受. 可以肯定, 从那时以来, 数学家们实际做出并发表的证明, 罕有使用完全形式化的文本的, 它们典型地表现为一种非常清晰的论证, 它们足够准确, 使得读者们相信可以 —— 原则上可以, 或者经过直截了当的努力 (如果足够持久的话) 就可以 —— 变成完全的形式化的文本. 然而, 几十年来, 这个占统治地位的思想受到的限制也逐渐地出现了, 关于什么才算是有效的数学论证的新概念, 也越来越多地为时下的数学实践所接受.

企图系统地追随这个思想, 使之达到完全发挥的地步, 使得把证明作成一种完全形式化纯粹按句法进行演绎论证, 这种观念会遇到严重的困难, 这是早前完全没有期望到的. 1920 年代早期, 希尔伯特和他的合作者们发展了一种充分展开的数学理论, 以 "证明" 为其主题, 就是把 "证明" 本身变成研究的主题. 这个理论, 事先预设了关于证明的形式概念, 是作为一个雄心勃勃的宏大纲领的一部分, 意在给

出算术的一个直接的**有穷的**相容性的证明, 而算术是被表示成一个形式系统的. 希尔伯特指出, 正如物理学家要研究他们用来做实验的仪器、哲学家要从事对于理性的批判一样, 数学家也应该能够分析数学证明, 而且要用严格的数学手段来做这件事. 大约在这个纲领启动十年左右, 哥德尔[VI.92] 提出了他的惊人的不完全性定理[V.15], 非常著名地表明了"数学真理" 和 "可证明性" 不是一回事. 事实上, 在任何一个相容的相当丰富的公理系统 (包括数学家典型地使用的公理系统) 中, 一定有不能证明的真数学命题. 哥德尔的工作意味着希尔伯特的有穷论纲领太乐观了, 但是它同时也清楚地表明了从希尔伯特的证明论中可以得到多么深刻的数学洞察.

一个密切相关的发展是出现了一些工作, 证明了有些重要的数学命题是不可判定的. 有趣的是, 这些貌似否定的结果, 产生出确定这种命题的真理性的合法基础的新思想. 例如, 科恩 (Paul Joseph Cohen, 1934 –2007, 美国数学家) 在 1963 年确定了连续统假设[IV.22 §5] 在集合论的通常的公理系统下既不能证明, 也不能否证. 绝大多数数学家干脆地接受了这个思想, 认为问题已经解决 (虽然不是按照原来预期的方式解决的), 但是还有一些当代的集合论专家, 著名的有 Hugh Woodin, 仍然坚持, 有很好的理由相信这个假设为**不真**. 为了论证这一点, 他们遵循的方法与证明的形式方法基本不同, 他们设计了新的公理, 证明这些公理具有他们非常想要的性质, 然后再证明它们蕴含了连续统假设不真 (关于这一点, 更详细的讨论可见条目集合理论[IV.22. §10]).

第二个重要的挑战来自许多数学领域里的重要的证明变得越来越长. 一个著名的例子是有限单群的分类[V.7], 它的证明是由许多数学家把整个证明分成了许多部分来进行的. 最后的论证, 如果放在一起, 将有一万页之多, 而且从 1980 年代早期就已经宣布证明完成以来, 已经发现其中有错误. 改正这些错误, 倒总是比较直截了当的事, 而这个定理已经被许多群论专家所接受和使用. 然而, 一个证明长到让单个个人无法检验, 这对于何时应该接受这样的证明, 甚至对于证明这个概念本身, 也是一个挑战. 更近一点, 费马大定理[V.10] 和庞加莱猜想[V.25] 这些非常显著的场合, 对它们很难作一个概述, 理由很多, 不仅是太长 (虽然完全没有有限单群的分类定理那么长), 而且太难. 在这两种情况下, 从第一次宣布证明, 到为数学界完全接受, 有很长的时间间隔, 因为要检验这些证明, 只有极少数的人有资格, 而即令他们也还要花极大的精力. 对于这两个突破都没有争议, 但是它们确实引起了一个社会学的问题: 如果有人宣称证明了一个定理, 而没有任何人准备细心地检验 (可能和上面提到的两个定理不同, 这一个定理对于别的数学家可能还没有重要到值得为它花上那么多的时间), 那么, 这个定理的状况算是什么样呢?[算是已经得到证明, 还是没有得到证明呢?]

在不同的数学领域里都出现了一些基于概率考虑的证明, 这里有数论、群论和组合学. 有时候能够证明一些数学命题, 但证明并不具有完全的确定性, 而只是证明了错误的概率极小, 例如最多是十万亿分之一 (例如参看条目*计算数论*[IV.3 §2] 中关于素性的随机检验的讨论). 在这样由情况下, 我们可能并没有一个形式证明, 但是把这个命题看成真命题, 我们犯错误的机会, 例如说, 大概也会小于在上面所说的那些很长的证明中找到一个值得注意的错误的机会.

另一个挑战来自引入了计算机辅助的证明. 例如, Kenneth Appel 和 Wolfgang Haken 在 1976 年通过证明*四色定理*[V.12] 解决了一个老问题. 他们的证明涉及对于为数巨大的不同映射构形分别加以检验, 他们借助于计算机完成了这件事情. 一开始, 这件事引起了一些辩论: 这样的证明是否合法? 但是这个证明很快就被接受了, 而且现在有好几个问题都是这样由计算机辅助证明的. 有些数学家甚至相信, 将来这种计算机辅助证明, 以及更重要的还有**计算机生成**的证明, 是数学整个学科的未来. 在这种观点 (目前还只是少数派) 之下, 我们现在关于什么是可接受的数学证明的观点都会变成陈腐的观点了.

最后一点需要强调的是, 许多数学分支现在都有一些猜想, 它们都具有基本的重要性, 但是在可以预见的将来, 证明它们还是人们力不能及的事. 相信这些猜想为真的数学家们越来越多地从事系统地研究这些猜想的推论, 假设在不远的时日可接受的证明会出现 (至少是相信这个猜想为真), 这种有条件的结果也被顶级的数学刊物接受发表, 而且博士学位也通常会颁发给他们.

所有这些潮流都对于一些现存的概念提出了有趣的问题. 这里就有: 合法的数学证明的概念、真理性在数学中的状况和地位、“纯粹” 和 “应用” 领域的关系, 等等. 对于证明的形式概念, 即认为证明只是一串符合某些句法规则的符号, 仍然为深藏的原理提供了理想的模型, 而绝大多数数学家仍然认为这些原理就是他们的学科的本质. 它对于某些公理系统的力量作出了含义深远的分析, 但同时, 数学家们在决定自己的专业实践中哪些算是合法的, 态度总在变化, 而又不能解释这些变化.

致谢 作者要感谢 José Ferreiróse 和 Reviel Netz 对本文以前各稿所作的有用的评论.

进一步阅读的文献

Bos H. 2001. *Redefining Geometrical11Exactness. Descares' Transformatons of the Early Modern Conception of Construction.* New York: Springer.

Ferreirós J. 2000. *Labyrinth of Thought. A History of Set Theory and Its Role in Modern Mathematics.* Boston, MA: Birkhāuser

Grattan-Guiness I. 2000. *The Search for Mathematical Roots: Logics, Set Therory and the Foundationgs of Mathematics from Cantor through Russell to Gödel.* Princeton, NJ:

Princeton University Press.

Netz R. 1999. *The Shaping of Deduction in Greek Mathematics: A Study in Cognitive History*. Cambridge: Cambridge University Press.

Rashed R. 1994. *The Development of Arabic Mathematics Between Arithmetic and Algebra*. Translated by Armstrong A F W. Dordrecht: Kluwer.

II.7 数学基础中的危机

Josê Ferreirós

数学基础的危机在数学家圈子里面是一件远近闻名的事情, 而且如雷贯耳, 已经到达很大的非数学听众之中. 大家都认为, 一个受到良好训练的数学家应该多少知道一点关于三种观点的事情, 就是“逻辑主义”、“形式主义” 和 “直觉主义”(下面再来解释), 还有关于数学知识的状况, 应该知道哥德尔的不完全性定理[V.15] 告诉了我们什么. 专业的数学家关于这类主题时常各有主见: 或者认为关于基础的讨论没有意义 —— 这样就站在多数人一边了, 或者对于数学持有某种形式的修正主义观点, 认为这是一个原则问题, 或者是很吸引人的事. 但是辩论历史的真实的概要则不甚为人所知, 与之相关的更微妙的哲学论题时常被忽略了. 本文中主要讨论前者, 即辩论历史的真实的概要, 使得有助于把主要的思想概念问题弄得更加明确.

数学基础的危机统通常被理解为 1920 年代发生的一件局部性的事情, 是两个 “党派” 之间的激烈争论. 一派是希尔伯特[VI.63] 领导的 “经典”(即已经过去的 19 世纪) 数学的拥护者; 另一派则是他们的批评者, 由布劳威尔[VI.75] 领导, 则主张对已为人所接受的教义作强烈的修正. 但是, 在我看来, 数学基础的危机还有第二个很重要的意义, “危机” 是一个漫长的全局的过程, 与现代数学的兴起以及它所创造的哲学的方法论问题是无法分辨开来的. 本文就是从这个观点出发写成的.

然而, 在这个比较长的过程中, 我们仍然可以挑选出一些值得注意的时间区间. 在 1870 年左右, 关于非欧几何的可接受性问题、关于复分析的适当的基础问题, 甚至关于实数的问题, 都有很多的讨论. 到了 20 世纪早期, 又有关于集合论、连续统概念、逻辑的作用以及公理方法与直觉的作用的对抗, 都有过辩论. 到了 1925 年, 则发生了本质意义的危机, 这时, 这些辩论里的主要思想都发展了, 变成了详尽的数学研究的主题. 到了 1930 年代, 哥德尔[VI.92] 证明了他的不完全性定理, 如果不放弃一些自己热爱的信念, 是不能消化这个结果的. 我们来比较详尽地分析一下这些事件和问题.

1. 早期的基础问题

有证据表明, 希尔伯特在 1899 年认可了一种观点, 这种观点后来被称为 “逻辑主义”. 逻辑主义就是这样一个论点: 数学的基本概念可以用逻辑概念来定义, 而数学的关键的原理仅需要逻辑原理就可以推导出来.

久而久之, 这个概念变得不那么清楚了, 似乎是基于逻辑理论的范围有多大, 人们具有的只是模糊而且不成熟的概念. 但是从历史上说, 逻辑主义是对于现代数学兴起的一种心智上很美妙的反应, 特别是对于集合论的途径和方法的反应. 因为多数人[①] 的意见是, 集合理论是 (精炼的) 逻辑的一部分, 所以这个论点似乎得到了自然数和实数理论可以从集合理论导出这一事实的支持, 也得到了集合论方法在代数和实的及复的分析中作用日益增大的支持.

在如何理解数学上, 希尔伯特是追随戴德金[VI.50] 的. 对于我们, 希尔伯特和戴德金的早期的逻辑主义的实质就是直觉地认可某些现代的方法, 不管它们当时看来如何大胆. 这些方法是在 19 世纪逐渐出现的, 特别是与哥廷根的数学相联系的 (高斯[VI.26]、狄利克雷[VI.36]); 哥廷根的数学由于黎曼[VI.49] 的崭新思想出现了至关重要的转折, 而由戴德金、康托[VI.54]、希尔伯特和其他一些比较小的人物进一步发展了. 同时, 有影响的柏林数学学派一直反对这个新潮流, 克罗内克[VI.48] 是公开正面反对, 魏尔斯特拉斯[VI.44] 则比较微妙 (魏尔斯特拉斯的名字和把严格性引入实分析是同义语, 但是事实上, 如下面将要指出的那样, 他并不赞成那时精心制作的更加现代的方法), 巴黎和其他地方的数学家们对于这些新的激进思想也多心存疑虑.

这种现代的途径的最具特征的显著特性是:

(i) 接受狄利克雷所提出的 “任意” 函数的概念;

(ii) 完全地接受无穷集合以及更高级的无穷大;

(iii) 愿意 “以思想代替计算”(狄利克雷), 而更关注于由公理所刻画的 “结构”; 还有

(iv) 时常依赖于 “纯存在” 的证明方法.

这些特性的一个有影响的早期的例子是戴德金处理代数数理论[IV.1] 的途径 —— 他对数域[III.63] 和理想[III.81. §2] 的集合论定义, 以及他证明诸如唯一分解的基本定理的方法. 戴德金用理想这种代数整数的无穷集合的概念来研究代数整数的因子分解性质, 引人注目地脱离了数论的传统. 利用这种新的抽象概念, 再加上两个理想的积的适当定义, 戴德金就能够完全一般地证明在代数整数的任意环中, 理想都可以唯一地分解为素理想的乘积.

①应该提到, 黎曼和康托这些关键人物并不同意 (Ferreirós, 1999). “多数人” 中包括了戴德金、佩亚诺[VI.62]、希尔伯特、罗素[VI.71] 等.

有影响的代数学家克罗内克抱怨戴德金的证明并没有使我们能够计算任何特例下的有关的除式即理想, 就是说, 这个证明是**纯粹的存在证明**. 克罗内克的观点是, 这种抽象的工作方法是由于集合论的方法和集中注意于相关的结构的代数性质, 才成为可能的, 这里算法的处理 ——即所谓**构造的方法**—— 是太遥不可及了. 戴德金则认为克罗内克的抱怨是无的放矢, 戴德金的成功在于他由于仔细贯彻"以思想代替计算"这个原则而取得了成功, 黎曼的复变函数理论也是强调了这个原则. 很明显, 具体的例子需要发展更精巧的计算技巧, 而戴德金的几篇文章都是为此目的的.

通过 1867–1872 年发表的文章, 黎曼和戴德金的思想和方法更加为人所知了. 这些文章特别使人震撼, 是因为它们非常公开地为一个观点辩护: 数学理论**不应该**以公式和计算为基础, 它们应该总是以表述清楚的**一般概念**为基础, 而把解析表达式和计算的工具推给理论的进一步发展.

为了解释这种对立, 让我们考虑黎曼和魏尔斯特拉斯对待函数论的不同途径的对立这个特别清楚的例子. 魏尔斯特拉斯把解析函数 (或称全纯函数[I.3 §56]) 显式地表示为幂级数 $\sum_{n=0}^{\infty} a_n(z-a)^n$ 的一个集合, 其元素互相以解析拓展[I.3 §56]相连接. 黎曼则选择了一个非常不同的更抽象的途径定义一个函数为解析, 如果它满足柯西–黎曼的可微分条件[I.3 §56][①]这个干净利落的定义是魏尔斯特拉斯所反对的, 因为可微分函数类从来没有被 (例如用级数表示) 仔细地刻画过. 魏尔斯特拉斯发挥了他的批评才能, 给出了一个连续但处处不可微分的函数的例子.

值得注意的是, 在更加偏好把无穷级数作为研究分析和函数论的关键工具这一点上, 魏尔斯特拉斯其实更加接近于 18 世纪把函数作为一个解析表达式的观点. 另一方面, 黎曼和戴德金总是赞成狄利克雷的抽象的观点, 即函数 f 是对于每一个 x 用一个任意的 $y=f(x)$ 与之相关的"任意"的办法 (在这以前, 曾经要求 y 应该通过一个解析表达式用 x 来表示). 魏尔斯特拉斯在一封信里, 批评过狄利克雷的这个概念太一般、太模糊, 不能成为有趣的数学研究的起点. 他似乎忘记了一件事, 那就是狄利克雷的这个观点正是定义和分析一些一般概念如连续性[I.3 §5.2] 和积分[I.3 §5.5] 的正确的框架. 在 19 世纪, 这个框架被称为**概念途径**.

在其他领域里也出现了类似的方法论的辩论. 克罗内克在 1870 年的一封信里走得这么远, 甚至说波尔扎诺–魏尔斯特拉斯定理是"明显的诡辩", 并且许诺自己会找到一个反例. 波尔扎诺–魏尔斯特拉斯定理宣布实数的有界无穷集合必有聚集点, 这是古典分析的基石, 而且正是魏尔斯特拉斯在他的著名的柏林讲义里这样肯定的. 克罗内克的问题在于实数系的完备性公理的 (这个公理的一种表述方法是,

①用一系列的特性来决定一个特定的函数, 例如用与之相关的黎曼曲面[III.79] 和在奇点处的性态. 这些特性则通过某个变分原理 (例如"狄利克雷原理") 来决定一个函数, 这一点也被魏尔斯特拉斯批评过, 他给出了一个反例. 希尔伯特和 Adolf Kneser(1862–1930, 德国数学家) 重新陈述和论证了这个条件.

$\mathbf{R}$ 中的每一个非空闭区间套必有非空交集). 实数不能够用初等方法从有理数构造出来, 为此必须严重地依赖于无穷集合 (例如应用 “戴德金分割”, 而所谓戴德金分割就是有理数集合的子集合 $C \subset \mathbf{Q}$, 使得当 p 和 q 都是有理数而且 $p < q$ 时, 由 $q \in C$ 必可得到 $p \in C$). 换一个方法来说, 克罗内克是要人们注意这样一个问题, 即波尔扎诺 — 魏尔斯特拉斯定理中的聚集点不能用初等方法从有理数构造出来, 这种情况是很常见的. 在实数集合, 即 “连续统” 这样经典的定义里面, 就已经包含了现代数学的**非构造**成分的种子.

到了 1890 年, 希尔伯特关于不变式论的工作又引起了关于另一个基本定理, 即基底定理的纯存在证明的一场辩论, 这个定理 (用现代的用语来说) 就是: 多项式环的每一个理想都是有限生成的. 哥尔丹 (Paul Albert Gordan, 1837–1912, 德国数学家) 因他关于不变式理论的繁冗的算法处理而著名, 人称 “不变式之王” 的他, 曾经幽默地讥讽希尔伯特的这项工作是 “神学” 而不是数学 (这明显地意味着希尔伯特的证明是纯粹的存在证明而不是构造性的, 就如同哲学中上帝的存在证明一样).

这种早期的关于基础的辩论的对立双方, 观点都逐渐清晰了. 康托在集合论中的证明方法也成了存在证明的现代方法论的精彩例子. 他在 1883 年的一篇论文里为高阶的无穷大和现代的方法论作公开辩护, 其中夹着对克罗内克的观点的辛辣的暗地批评. 另一方面, 克罗内克早在 1882 年就公开批评过戴德金的方法, 又私下反对康托, 而到了 1887 年则著文详细说明自己关于基础的主张. 戴德金则在 1888 年用详细的关于自然数的集合理论 (在他本人看来, 这就是逻辑主义了) 作答.

早一轮的互相批评以现代派阵营的胜利告终, 这时, 这个阵营又增加了新的盟友, 如赫尔维茨 (Adolf Hurwitz, 1859 – 1919, 德国数学家)、沃尔泰拉 (Vito Volterra, 1860 –1940, 意大利数学家)、佩亚诺和*阿达玛*[VI.65], 还有*克莱因*[VI.57] 这样有影响的人物为它撑腰. 虽然黎曼的函数论还有待改进, 在实分析、数论和其他领域的新进展则都在表现出现代方法的力量和前景. 到了 1890 年代, 一般说来是现代观点, 特别是逻辑主义, 得到了很大的发展. 希尔伯特把这种新的方法论发展成为公理方法, 非常有效地用于几何学 (1899 年出版了他的《几何基础》, 以后又发行了多版) 以及实数系的研究.

然后, 突然出现了所谓逻辑悖论[①]. 康托、罗素、策墨罗 (Ernst Friedrich Ferdinand Zermelo 1871–1953, 德国数学家) 和许多其他人都发现了悖论. 对此, 下面还要讨论. 悖论有两类: 一类是有一些用以表明某些集合存在的论证会引起矛盾, 这一类称为**集合论的悖论**; 另一类是有些论证说明了在真理和可定义性的概念中也会有困难, 这一类称为**语义悖论**. 这些悖论的出现, 完全摧毁了逻辑主义所提出的关

①关于逻辑悖论, 可以参看《现代世界中的数学》一书中蒯因所写的: “**悖论**” 一文 (齐民友等译, 上海教育出版社, 2004 年出版, 331-346 页).—— 中译本注

于数学的新近发展的吸引人的观点. 说真的, 逻辑主义的全盛时期是在悖论出现**以前**, 即 1900 年以前; 后来还因为罗素和他的 "类型理论" 有复兴之势, 但是, 到了 1920 年左右, 对逻辑主义更有兴趣的是哲学家而不是数学家. 现代方法的拥护者和构造主义批评者的分裂等在那里.

2. 1900 年左右

希尔伯特以康托的*连续统问题*[IV.22 §5] 来开始他在 1900 年巴黎的第一届世界数学家大会上的著名问题清单, 这是集合理论的一个关键问题, 而接着的第二问题就是是否每一个集合都可以良序的问题. 第二问题相当于确立实数集合 $\mathbf{R}$ 的概念为相容的. 他用这两个问题来开始不是偶然的, 可以说这是一个对于 20 世纪的数学应该是怎么样的作清楚的宣示的办法. 这两个问题, 还有他的年轻的同事策墨罗用来证明 $\mathbf{R}$(即连续统) 可以良序的*选择公理*[III.1], 是上面列出的特性的清单 i — iv的例子中的精华. 毫不奇怪, 那些不那么胆大的人就起来反对, 复活了克罗内克的怀疑, 这一点可以从 1905–1906 年发表的许多论文看出来. 这就把我们带到辩论的下一个阶段.

2.1 悖论和相容性

当事件发生了引人注目的转折时, 现代数学的冠军们在一些论证上面摔了跤, 使人对他们的论证是否中肯产生了新的疑虑. 到了 1896 年前后, 康托发现所有序数的集合和所有基数的集合, 这些表面上无害的概念都会导致矛盾. 在序数的情况, 这个矛盾通常称为**Burali-Forti**(Cesare Burali-Forti, 1861–1931, 意大利数学家)**悖论**, 而在基数情况, 则称为**康托悖论**. 按照康托前面的结果, 所有序数形成一个集合这一假设, 将会导致存在一个序数小于其自身 —— 对于基数, 也有类似的结果. 戴德金在听说这些悖论以后, 开始怀疑人类的思想是否完全是理性的. 更糟的是, 在 1901 年或 1902 年, 策墨罗和罗素发现一个很初等的矛盾, 现在称为**罗素悖论**, 有时也称为**策墨罗– 罗素悖论**, 这一点我们马上就要来讲. 现在已经很清楚了, 把集合理论理解为逻辑是站不住脚的, 一个新的不稳定的时期开始了. 但是应该说, 只有逻辑学家心烦意乱, 因为矛盾是出现在他们的理论中.

现在我们来解释策墨罗–罗素悖论的重要性. 从黎曼到希尔伯特, 许多作者都接受了一个原则: 给定任意的适当定义的逻辑或数学性质, 必定存在一个集合, 即所有具有这个性质的元素的集合. 用符号来表示, 设有一个适当定义的性质 p, 则必存在另一个对象, 即集合 $\{x : p(x)\}$. 例如, 相应于 "是一个实数" 这个性质 (这个性质已经用希尔伯特的公理形式化了), 就有所有实数的集合; 相应于 "是一个序数" 这个性质, 就有所有序数的集合, 如此等等. 这就称为**概括原理**, 它是对于集合的逻辑主义理解的基础, 这样理解的集合论称为朴素集合论, 虽然其朴素性是后来

才看出来的. 这个原理被认为是一个基本的逻辑法则, 所以, 整个集合理论只不过是初等逻辑的一部分.

策墨罗–罗素悖论表明, 概括原理是会引起矛盾的, 要想说明这件事, 只需陈述一个看起来尽可能基本、尽可能属于纯粹逻辑的性质. 令 $p(x)$ 为 $x \notin x$ 这个性质 (记住, 否定和元素关系都假设为纯粹的逻辑概念). 于是, 概括原理给出了集合 $R=\{x: x\notin x\}$ 的存在性. 但是这里可就引起了矛盾: [R 是否 $\in R$?], 如果 $R\in R$, 则由集合 R 的定义, 应有 $R\notin R$. 与此类似, 如果 $R\notin R$, 则应有 $R\in R$. 希尔伯特 (像他的年长的同事弗雷格[VI.56] 一样) 被迫放弃逻辑主义, 他甚至怀疑, 克罗内克是否一直是正确的. 最后, 他得到一个结论: 集合论表明, 有必要修正逻辑理论. 有必要用公理化的方法来建立集合论, 使之成为一个基于数学公理 (而不是逻辑公理) 的基本的**数学理论**, 策墨罗就来从事这项工作.

希尔伯特为这样一个主张辩护: 想要宣称数学对象的某个集合是存在的, 就等于要证明相关的公理系统是相容的, 即是无矛盾的. 这个主张是很有名的, 有文献证据表说明, 这个著名的主张是对康托悖论的回应. 他的推理可能是这样的: 不能直接从适当定义的概念马上就跳到相应的集合, 而要先证明这些概念是逻辑相容的. 例如, 要想接受实数集合, 就要先证明关于实数的希尔伯特公理系统是相容的. 希尔伯特的原理是从数学存在的概念里清除一切形而上学的内容的方法. 这样一个观点, 即数学对象有一种在思想领域里的 "理想的存在性", 而没有一种独立的形而上学的存在性, 这是戴德金和康托早就期望的.

"逻辑" 悖论不仅是包括了以 Burali-Forti、康托和罗素命名的那些悖论, 还有许多语义悖论, 由罗素、理查德 (Jules Antoine Richard, 1862–1956, 法国数学家)、柯尼希 (Julius (Gyula) König, 1849–1913, 匈牙利数学家, Julius 在匈牙利文中就是 Gyula)、Grelling (Kurt Grelling, 1886 –1942, 德国数学家) 等许多人发现 (下面将要讨论理查德的悖论). 由于不同的悖论太多, 出现了不少的混乱, 但是有一件事很清楚: 悖论在促进现代逻辑学的发展和使数学家明白把他们的理论严格的形式化的重要性. 只有当一个理论用精确的形式语言表示出来以后, 才能不顾这些语义悖论, 而且把语义悖论与集合论悖论的区别陈述出来.

2.2 直谓性

当 1903 年弗雷格和罗素的书使得集合论的悖论为数学界广泛知晓时, 庞加莱[VI.61] 利用这些悖论对逻辑主义和形式主义提出了批评.

他对悖论的分析引导他造出了一个新概念: **直谓性,** 并且坚持在数学中必须避免非直谓的定义. 非形式地说, 一个定义是非直谓的, 如果它在引入一个元素时, 已经参照了一个整体, 而这个整体已经包括了这个元素. 下面是一个典型的例子: 戴德金定义自然数集合 **N** 为这样的集合之交, 这些集合都包含 1, 而且在下面的单射

函数 σ 下是闭合的, 这里 $1 \notin \sigma(\mathbf{N})$(函数 σ 称为**后继者函数**). 他的思想是把 $\mathbf{N}$ 刻画为最小的集合, 所以在他的程序中, 集合 $\mathbf{N}$ 是参照许多集合的整体来定义的, 但是这个整体中的每一个集合都已经包含了 $\mathbf{N}$. 所以, 这种程序是庞加莱所不能接受的 (罗素也不会接受), 只要是当有关的对象**只能**参照包含更多的整体才能定义时, [他们都不会接受]. 庞加莱在他研究过的悖论里都找到了非直谓的程序.

现在举理查德悖论为例. 这是一个有关语言的悖论, 即语义悖论 (我们说过, 在语义悖论中真理性和可定义性起了重要的作用). 我们从可定义的实数这个概念开始. 因为定义一定要用某种语言里的有限表达式来表出, 所以只有可数多个可定义数. 事实上, 我们可以按照其定义式的字母顺序把可定义数排列成表 (这种次序称为**字典顺序**). 理查德的思想是: 对可定义数的这个表, 应用康托证明 $\mathbf{R}$ 为不可数集合[III.11] 时所用的对角线程序. 令可定义数为 $a_1, a_2, a_3, \cdots$. 现在我们用系统的方法来定义一个数 r, [当然 r 也就成了一个可定义数], 但是我们可以使 r 的十进展开式的第 n 个数码与 a_n 的第 n 个数码不同 (例如当 a_n 的第 n 个数码不是 2 时, 就规定 r 的第 n 个数码为 2, 如果 a_n 的第 n 个数码是 2, 则规定 r 的第 n 个数码为 4), [这样, r 就与所有的 a_n 都不同], 从而 r 不可能成为可定义数. 但是这个构造的过程已经说明 r 是一个可以用有限多个字来定义的数! 庞加莱禁止使用非直谓的定义, 当然会阻止定义 r, 因为在定义它的时候是参照了所有可定义数的①.

在这种对待数学基础的途径下, 所有的数学对象 (凡超过了自然数的) 都必须用显式定义来引入. 如果一个定义涉及到预先假设的一个总体, 而想要定义的对象又是这个总体的一员, 就陷入了一个循环: 对象本身是其定义的组成部分. 按照这种观点来看, "定义" 必须是直谓的: 只能参照在定义这个对象以前就已经确定了的总体. 重要的作者如罗素和外尔[VI.80] 都接受这个观点, 而且发展了它.

策墨罗没有被说服, 他争论说, 非直谓的定义时常用起来很容易, 并不复杂, 不仅是在集合论中 (如戴德金关于 $\mathbf{N}$ 的定义) 有, 而且在古典分析中处处都有. 作为一个例证, 他引用了柯西[VI.29] 关于代数的基本定理[V.13] 的证明②, 但是非直谓定义还有一个更简单的例子, 即实分析中的最小上界 (亦即上确界). 实数并不是分别引入的, 即不是一个一个地各用一个直谓定义显式给出的, 而是作为一个完成了的整体给出的, 而从一个无穷的实数集合分出其最小上界的特定的方法就变成了非直谓的. 策墨罗坚持这些定义并无大害, 因为被定义的对象并不是由定义 "创造" 出来的, 而只是分离出来的 (见文集 (Heijenoort, 1967) 中策墨罗的论文, 183-198).

庞加莱关于废除非直谓定义的思想, 对于罗素是很重要的. 罗素把庞加莱的思

①现代的解决方法是在一个适当决定的形式理论之内来建立数学定义, 这个形式理论的语言和表达式在一开始就规定好. 理查德的悖论就是钻了可以容许的定义的手段是什么还有含混之处这个空子.

②柯西的推理明显是非构造的, 即是我们所说的 "纯存在" 证明. 为了证明多项式有根, 柯西研究了它的绝对值, 它有一个整体最小值. 这个整体最小值的定义是非直谓的. 柯西假设它为正, 由此得到一个矛盾.

想凝聚成他的类型理论中的所谓 “邪恶循环原理”(vicious circle principle). **类型理论**是一个高阶逻辑系统, 其中, 量词可以用于性质或集合、关系、集合的集合, 等等. 粗略地说, 它是基于这样一种思想: 一个集合的所有元素都应该是属于同一匀齐的类型的对象. 例如, 我们可以有 “个体” 的集合如 $\{a, b\}$, 可以有个体的**集合**之集合, 如 $\{\{a\}, \{a, b\}\}$, 但绝不可以有**混合的**集合如 $\{a, \{a, b\}\}$. 罗素版本的类型论, 后来由于他采用了所谓分支 (ramification) 以避免非直谓性而变得很复杂. 这个系统加上无穷公理、选择公理和 “化约公理”(这是一个人为造作得惊人的使得分支得以 “坍塌” 的手段), 就足够来发展集合论和数的系统了. 所以, 这就成了罗素和怀特海 (Alfred North Whitehead, 1861–1947, 英国逻辑学家、数学家和哲学家) 的巨著《数学原理》(*Principia Mathematica*, 1910–1913, 共三卷. 以下简称《原理》) 的逻辑基础. 罗素和怀特海在这部巨著里发展了一个数学基础.

直到 1930 年左右, 类型理论都是主要的逻辑系统, 但是这是指的简单类型理论 (即没有分支的类型理论), 正如 Chwistek (Leon Chwistek , 1884 – 1944, 波兰逻辑学家)、拉姆齐 (Frank Plumpton Ramsey, 1903 –1930, 英国数学家、逻辑学家) 和其他人所已经认识到的那样, 这些对于《原理》那种风格的数学基础已经足够了. 拉姆齐提出的论证指向消除对于非直谓性的担心, 他还试图论证《原理》中的其他存在公理 —— 如无穷公理和选择公理 —— 都是逻辑原理. 但是他的论证并不是结论性的. 罗素想把逻辑主义从悖论下解救出来的企图仍然不足以服人, 只有少数几个哲学家 (特别是所谓 “维也纳学派”[①]除外).

庞加莱的建议也是外尔的《连续统》(*Das Kontinuum*) 一书的关键原理. 外尔在这本书里提出了有趣的研究数学基础的途径. 外尔的思想是接受常规的、用经典逻辑发展起来的自然数理论, 但是再向前走, 就要按照直谓性的要求来工作了. 这样, 外尔和布劳威尔不同, 他接受排中律 (这件事和布劳威尔的观点将在下一节讨论). 然而, 他不能使用完全的实数系统: 在他的系统中, 实数集合还不是完备的, 波尔扎诺 — 魏尔斯特拉斯定理也是不成立的. 这就是说, 他还必须想出非常精巧的方法来代替分析中的结果的常用的推导.

按照外尔风格的数学的直谓的基础, 最近几十年里有很值得注意的结果 (Feferman, 1998). 直谓系统介于赞成所有现代方法论的系统和约束很紧的构造主义系统之间. 有好几个系统都不适合通常的但是现在已经过时的逻辑主义、形式主义和直觉主义的三分天下, 外尔的系统是其中之一.

①“维也纳学派”, 人们更经常称为 “维也纳小组” (Vienna Circle). 当时围绕着哲学家石里克 (Moritz Schlick) 的一群哲学家, 组织了一个会社名为马赫学会 (Verein Ernst Mach), 其成员有哥德尔和一批与数学关系密切的 (特别是与哥廷根的数学) 的哲学家, 人们就称他们为维也纳学派. —— 中译本注

2.3 选择

悖论虽然很重要, 但它们对于关于基础的辩论的影响被夸大了. 人们常可找到一些文章, 以悖论作为这场辩论的真正起点, 这与我们在第 1 节里的说法成了鲜明的对照. 但是, 即令我们限制只考虑 20 世纪的第一个十年, 也还有一场争论, 其重要性并不稍次, 这就是围绕着选择公理和策墨罗对良序定理的证明的争论.

回忆一下, 我们在 2.1 节里说到的集合和定义此集合的性质之间的关联, 在当时数学家和逻辑学家的脑海里已经是根深蒂固的了 (通过矛盾的概括原理). 选择公理 (以下简记为 AC) 是这样一个原理, 它指出, 给定任意的一族无穷多个互相分离的非空集合, 必存在一个集合, 称为**选择集合**, 其中含有族中每一个集合的恰好一个元素. 批评者说, 关于选择集合, 问题在于 AC 只保证了这个集合的存在, 而没有给出定义它的性质. 说真的, 如果能够显式地刻画选择集合, 也就可以避免使用 AC 了. 但是在策墨罗的良序定理的情况, 使用 AC 又是很本质的. 所需要的 $\mathbf{R}$ 的良序的存在性, 是在康托、戴德金和希尔伯特的 "理想" 意义下的存在, 似乎很清楚, 它完全没有构造主义的前景.

这样, 选择公理使得集合理论过去的概念更加模糊了, 迫切需要数学家对它作出澄清. 一方面 AC 只不过是**任意**子集这个老概念的一个显式的表示. 另一方面, 它又和人们强烈持有的必须用性质来显式地定义无穷集合有明显的冲突. 深刻的辩论的舞台已经搭好了. 关于这个特定主题的讨论, 在澄清现代数学方法在存在问题蕴含了什么意义上, 贡献更超过任何其他问题. 一件有教益的事情是知道波莱尔[VI.70]、贝尔 (René-Louis Baire, 1874 – 1932, 法国数学家)、勒贝格[VI.72](他后来成了一位批评者) 在证明分析中的定理时, 都不太明显地应用了 AC. 毫不偶然, 这个公理是由分析学家、希尔伯特的学生施密特 (Erhard Schmidt, 1876 –1959, 德国数学家) 向策墨罗提出的[①].

在策墨罗发表了他的证明以后, 在全欧洲都引起了热烈的辩论. 策墨罗被驱使去建立起集合理论的基础, 试图表明他的证明可以在一个无例外的公理系统中展开, 结果就是他的著名的集合理论的公理系统[IV.22 §3], 这是对于历史上由康托、戴德金和他自己的定理所贡献的集合理论进行仔细的分析而产生的杰作. 后来由弗朗克尔 (Abraham Halevi (Adolf) Fraenkel, 1891–1965, 德国数学家) 和冯 · 诺依曼[VI.91] 加以补充 (增加了代换公理和正规性), 又有外尔和斯科伦[VI.81] 提出的主要创新 (在一阶逻辑[IV.23 §1] 内陈述这个公理系统, 即只对个体和集合使用量词, 而不对性质使用量词), 到了 1920 年代, 这个公理系统就成了我们现在所知道的样子. [因为弗朗克尔的参加, 现在这个公理系统就简记为 ZF 公理系统].

---

①读一下法国分析学家在 1905 年的往返信件 (Moore, 1982; Ewald, 1996) 以及策墨罗在他 1908 年给出的良序定理的第二个证明 (Heijenoort, 1967) 时的聪明的论证, 至今仍旧会给出很多洞察.

ZFC(就是 ZF 加上选择公理) 把现代的数学方法论编为法典, 给出了发展数学理论和进行证明的令人满意的框架. 特别是它包含了很强的存在原理, 允许非直谓定义和任意函数, 允许纯存在证明, 而且使得有可能定义主要的数学结构. 这样, 它就展现了第 1 节里提出的趋势 i—iv. 策墨罗自己的工作完全符合希尔伯特在 1900 年时的非形式的公理化, 他也没有忘记许诺可以给出相容性的证明. 公理化集合论, 不论是 ZF 的表示, 还是冯 · 诺依曼 — 伯奈斯 (Paul Isaac Bernays, 1888–1977, 瑞士数学家)— 哥德尔的形式, 都是绝大多数数学家认可的自己学科的工作基础.

说到 1910 年代, 罗素的类型理论和策墨罗的集合理论的对立是很强的. 前者一是在形式逻辑下发展的, 二是它的出发点是与直谓主义完全一致的 (虽然后来有一些为求实效的理由, 使它作了一些妥协). 为了导出数学, 这个系统需要无穷大存在的假设和选择, 但是只是用一些修辞的处理, 把它们当成试探性的假设, 而不是当作堂而皇之的公理. 后一系统则不同：一是它是非形式地表述出来的, 二是它一心一意地采用了非直谓的观点, 而且把足够导出全部古典分析和康托的高阶无穷大理论所需的强存在假设都当作公理. 到了 1920 年代, 在这两个特性上的分歧大大地减少了. 策墨罗的公理系统被完善了, 而且是用现代的形式逻辑的语言来表述了. 罗素派则采用了简单类型理论, 这样接受了现代数学的非直谓的和关于 "存在" 的方法论. 罗素派也因此获得了 "柏拉图主义" 的名声 (虽然潜在有混淆的危险), 这个理论所讲到的对象, 都**好像**是独立于数学家能否真正显式地加以定义的.

就在这一段时间里, 再追溯到 20 世纪的第一个十年, 一个年轻的数学家在荷兰开始追求构造主义的一种带有哲学色彩的版本. [他就是*布劳威尔*[VI.75]]. 布劳威尔在 1905 年提出了他的非常特别的形而上学和本民族特有的观点, 而且在他的 1907 年的论文中开始详细阐述相应的数学基础. 他的 "直觉主义" 的哲学来自一个古老的形而上学观点：个体的意识是知识的唯一来源. 这种哲学本身可能没有什么意义, 所以我们在此只关注布劳威尔的构造主义原理. 在 1910 年左右, 布劳威尔已经是一个有名的数学家了, 在拓扑学上有关键性的贡献, 如他的*不动点定理*[V.11]. 到第一次世界大战末, 他开始发表文章详细阐述他关于数学基础的思想, 这就帮助创造了著名的 "**危机**", 我们马上就要转到这个问题上来. 他还在确立形式主义和直觉主义的区别的现行的 (但是是误导的) 看法上也很成功.

3. 严格意义下的危机

1921 年,《数学杂志》(*Mathematische Zeitschrift*) 发表了著名数学家外尔的一篇文章, 外尔是希尔伯特的弟子, 现在公开地赞成直觉主义, 诊断数学患上了 "基础的危机". 这个危机指出分析的老状况正在 "解体", 危机是由于布劳威尔的 "革命" 而来的. 外尔的这篇文章, 本意在于作为一本宣传小册子, 想唤醒 "沉睡的人", 这一点它确实做到了. 同年, 希尔伯特作答, 攻击布劳威尔和外尔想发动一场 "政

变”(putsch), 企图建立 “克罗内克式的专政”(见 (Mancosu, 1998) 和 (van Heijenoort, 1967) 中的相关文章). 关于基础的辩论急剧地变成了希尔伯特想要为 “经典的” 数学作论证和布劳威尔正在发展的重建一种经过了重大改革的直觉主义数学之战.

布劳威尔为什么成了 “革命党人”? 直到 1920 年, 关键的基础问题一直是实数可否接受的问题, 以及更为基本的非直谓性以及集合论中的强存在假设可否接受的问题, 正是非直谓性和这些假设, 支持了高阶的无穷大以及无限制地使用存在证明. 集合理论以及由此而蕴含着古典分析, 一直由于依赖于非直谓定义和强存在假设而遭到批评 (特别是选择公理, 谢尔品斯基 [VI.77] 在 1918 年就广泛地使用了它). 这样, 在 20 世纪的头 20 年, 辩论集中在这样一个问题上: 在涉及定义集合和它们的子集合并确定它们的存在时, 接受和允许使用哪些原理? 一个关键问题是, 怎样把 “任意子集合” 这种说法后面的模糊的含义弄严格? 对于这个问题, 最为前后一贯的反应是策墨罗的把集合论公理化, 以及外尔在《连续统》一书中的直谓系统 (罗素和怀特海的《原理》是直谓主义和经典数学中间的不成功的妥协).

然而, 布劳威尔把新的甚至更基本的问题带到了前台. 以往, 没有人曾经对关于自然数的传统推理方式起过疑问; 对于古典逻辑的使用, 特别是量词和排中律在这个背景下的使用, 谁也没有犹豫过. 但是, 布劳威尔对于这些假设提出了原则性的批评, 并且开始发展一种比外尔还激进得多的另一种分析理论. 在这样做的时候, 他突然生成了一种新的连续统理论, 正是这个理论最终俘获了外尔, 促使他宣布新时代的来临.

3.1 直觉主义

关于 “直觉主义集合论”, 布劳威尔用德文写了两篇文章来系统地发展他的观点. 这两篇文章分别于 1918 年和 1919 年发表在荷兰科学院的 *Verhandelingen* 上. 这些贡献是他后来说的直觉主义的 “第二幕” 的一部分. “第一幕”(从 1907 年开始) 则是强调数学的直觉基础. 克莱因和庞加莱就一直坚持直觉在数学知识中有着不可逃避的作用, 尽管逻辑在数学证明和发展数学理论上很重要, 数学却不能归结为纯粹的逻辑; 理论和证明当然要按逻辑组织起来, 但是它们的基本原理 (即公理) 是建立在直觉的基础上的. 但是布劳威尔走得比他们更远, 他坚持数学对于语言和逻辑是绝对独立的.

从 1907 年起, 布劳威尔就反对排中律 (principle of the excluded middle, 后来就用这几个字的首位字母 PEM 代表排中律), 认为它等价于希尔伯特的每一个数学问题都可解这一信念. PEM 是这样一个逻辑原理: 不论 p 表示什么命题, 命题 $p \vee \neg p$(即 p 或者非 p) 总是真的 (例如, 由 PEM 或者 π 的十进展开式中有无穷多个 7, 或者只有有限多个 7, 虽然我们不知道证明哪一个). 布劳威尔认为, 我们所习惯的逻辑原理都是从我们处理有限集合的子集合的方法中抽象出来的, 所以把它们

也用于无穷集合的情况是不对的. 在第一次世界大战以后, 他就开始来系统地重建数学.

直觉主义者的立场是, 只有当我们或者能够给出 p 的一个构造性的证明, 或者能够给出 q 的一个构造性的证明, 这时才能说 "p 或者 q". 这个观点有一个推论, 即归谬法 (reductio ad absurdum) 是无效的. 考虑希尔伯特的基底定理 (见 §1) 的第一个证明, 它就是由 reductio 给出的. 他证明了假设基底为无限会导致矛盾, 由此他就得到基底为有限的. 这个程序后面的逻辑就是从 PEM $p \vee \neg p$ 的具体例证开始, 证明 $\neg p$ 是站不住脚的, 而得出结论, 即 p 一定为真. 但是, 直觉主义者要求对于每一个假设为存在的对象, 都要给出**显式的**构造程序, 要给出每一个数学命题后面的显式的程序. 类似于此, 我们曾经提到柯西关于代数的基本定理的证明 (§2.1), 还有实分析中许多用到上确界的证明. 所有这些证明对于直觉主义者都是无效的. 例如, 外尔和 Kneser 都从事过代数学的基本定理的构造性证明.

很容易给出直觉主义者不会接受的应用 PEM 的例子, 只需要把 PEM 用于任意未解决的数学问题就行了. 例如, 所谓卡塔兰 (Catalan) 常数就是

$$K = \sum_{n=0}^{\infty} \frac{(-1)^n}{(2n+1)^2}.$$

不知道 K 是否超越数, 所以, 如果 p 表示以下命题: "卡塔兰常数是超越数", 则直觉主义者不会接受 p 或真或不真这一点.

这可能有点怪, 甚至显然是错的, 除非我们认识到, 直觉主义者对于什么是真也有不同的观点. 对于一个直觉主义者, 说一个命题为真, 就**意味着**我们可以用正在讨论的这种约束很紧的方法来证明它; 说它不真, 就**意味着**能够实实在在地找出它的反例. 因为没有理由假设或者有一个构造性的证明, 或者有显式的反例, 所以我们没有理由相信 PEM(按照对于真的这种理解). 这样, 为了确定具有某个性质的自然数存在, 用归谬法去证明是不够的. 如果想说服一位直觉主义者, 就得要用显式的确定方法来证明它.

请注意这个观点是怎样蕴含着数学并非与时间无关, 并非非历史的. 到了 1882 年, 林德曼才证明了 π 是一个*超越数*[III.41]. 按照直觉主义者的说法, 直到那时对于 [π 为超越数] 这个命题才可以赋以一个真值, 而 [在 1882 年] 以前, 按照直觉主义者的看法, 这个命题却是一个既不为真又不为不真的命题. 这听起来像是怪论, 但是对于布劳威尔, 这可是正确的, 因为在他看来, 数学对象是心智的创造, 而他认为说数学对象有独立的存在性只不过是 "形而上学" 罢了.

1918 年, 布劳威尔把康托和策墨罗的集合代之以构造主义的对应物. 后来, 布劳威尔把这种对应物称为 "spread" 和 "species". 一个 "species" 基本上就是一个由特征的性质定义的集合, 但有一个前提, 即其每一个元素以前都已经用显式的构造

方法独立地定义了. 特别是, 每一个给定的 "species" 的定义都是严格直谓的.

"spread" 的概念特别具有直觉主义的特性, 它是布劳威尔的连续统定义的基础. 它的企图是避免理想化, 并且公正对待和充分利用数学构造依赖于时间的本性. 例如, 假设我们想要定义一个有理数序列来越来越好地逼近 2 的平方根. 在古典分析中, 我们把这个序列构思为整体存在的, 但是布劳威尔定义了一个他称为**选择序列**的概念, 更多地关注于这个序列可能是怎样形成的. 生成这种序列的方法之一是给出一个公式, 例如一个递推关系式: $x_{n+1}=\left(x_n^2+2\right)/2x_n$(还有初始值 $x_1=2$). 但是另一个方法是作一个服从于某些限制, 但不那么刚性决定的选择, 例如可以坚持 x_n 的分母为 n, 而分子要选得使 x_n^2 与 2 之差不超过 $100/n$, 这并不能唯一地决定 x_n, 但是确能保证这个序列会产出对于 $\sqrt{2}$ 的越来越好的逼近.

所以, 并不要求一个选择序列在一开始就已经完全确定了, 而可以包括数学家在不同的时刻再做选择的自由. 这两个特点使选择序列和经典分析里的序列大不相同. 有人说过, 直觉主义者的数学是 "创造中的数学". 与此对照, 经典数学是以一种与时间无关的客体性为标志的, 因为它的对象自身是完全确定而与数学家的思维过程无关的.

一个 "spread" 以选择序列为其元素 —— 它有点像一个规范序列如何生成的规则[①]. 例如可以取一个由所有选择序列生成的 "spread", 但这些序列要以特殊的方式开始, 这样一个 "spread" 代表一个线段 —— 一般说来 "spread" 不表示孤立的元素. 布劳威尔利用元素是满足柯西条件的选择序列这样的 "spread" 来作**连续统的**新数学概念, 连续统不再是由具有先前决定的具有柏拉图式的存在性的点 (或实数) 构成的. 它更加是真正 "连续" 的. 有趣的是这个观点使人想起了亚里士多德, 他在 2300 年前就已经强调连续统的优先性, 而拒绝一个延伸的连续统可以由无延伸的点构成这个思想.

布劳威尔对分析的重新发展的下一个阶段是对函数概念的分析. 布劳威尔定义一个函数就是对一个 "spread" 的各个元素都指定一个值. 然而, 由于 "spread" 的本性, 这种指定的方法必须完全依赖于选择序列开始的一段, 这样才能是构造上可允许的. 这给出了一个很大的惊异: 所有处处定义的函数都是连续的 (甚至是一致连续的). 你可以怀疑, 对于下面的函数怎么办呢? 这个函数 f 就是当 $x<0$ 时 $f(x)=0$, 而 $x\geqslant 0$ 时 $f(x)=1$ 的函数. 对于布劳威尔, 这个函数不是一个适当定义的函数, 其深藏的理由在于我们可以定义 "spreads" 而不知道它们是正、是负或者是零 (可能永远也不会知道). 例如, 可以令 x_n 为 1, 如果在 4 和 $2n$ 之间的偶数

①严格地说, 一个 "spread" 是由两个规则生成的, 见 (Heyting, 1956) 或较近的 (van Atten, 2003), 其中有这一点和其他的细节. 可以把 "spread" 看成是自然数的万有树 (由自然数的所有有限序列构成) 的一个子树, 而对每一个节点都指定一个以前得到的数学对象. "spread" 有一个规则决定了树的节点, 另一个规则把这些节点映射到对象.

都是两个素数之和, 否则就定义 x_n 为 -1.

拒绝 PEM 有一个后果, 就是直觉主义的否定与经典的否定是不同的. 这样, 直觉主义的算术也和经典的算术不同. 然而, 哥德尔和根岑 (Gerhard Karl Erich Gentzen, 1909–1945 , 德国数学家) 在 1933 年证明了算术的**戴德金–佩亚诺公理系统**[III.67]**相对于**形式化的直觉主义算术是相容的 (就是说, 他们能确定在两个形式系统的语句之间有一个对应关系, 使得经典算术中的矛盾必然对应于其直觉主义对应物的一个矛盾. 因此, 若后者是相容的则前者也是). 这是希尔伯特派的一个小胜利, 虽然对于分析的系统和集合理论, 相应的证明一直没有得到.

在一开始, 人们寄希望于直觉主义最终会给纯粹数学一个简单而又优雅的表示. 然而从布劳威尔的重建在 1920 年代的发展越来越清楚, 直觉主义的分析将是极端复杂而又陌生的. 布劳威尔并不烦恼, 他在 1933 年说 "真理的球不会如幻想的球那样透明". 但是, 外尔虽然相信布劳威尔已经把数学直觉的领域整理得完全令人满意了, 却在 1925 年说: "数学家们痛苦地看到, 他们高耸入云的理论的最大部分在自己眼前化为烟云." 外尔似乎不久以后就放弃了直觉主义. 幸运的是还有另外一种途径, 建议了另外一种恢复经典数学的健康的方法.

3.2 希尔伯特的纲领

这里说的另外一种方法当然就是希尔伯特纲领. 就数学的经典理论而言, 这个纲领许诺的就是, 用他自己在 1928 年说过的值得纪念的一句话来说, "让一切疑虑一劳永逸地从世界上消除". 他从 1904 年起就开始发展的这个新的前景, 严重地依赖于形式逻辑和对可以从已给的公式 (即公理) 证明的公式作组合学的研究. 用现代逻辑学的方法, 证明变成了一种形式计算, 而可以机械地检验, 所以这个过程完全是构造性的.

按照前面讨论 (第 1 节) 的观点看来, 有趣的是, 这个新的计划是用克罗内克式的手段来论证现代的反克罗内克式的方法论. 希尔伯特的目的是证明从公理开始, 不会证明出矛盾的公式. 一旦能够组合地或者说构造地 (或者按希尔伯特自己说的有穷论 (finitarily) 地) 证明了这件事, 这里的论证就可以看成是对这个公理系统的论证 —— 哪怕我们从这个公理系统看到了所谈的是非克罗内克式的对象, 如实数系或者超限集合, [也可以用这种克罗内克式的手段来论证].

然而, 希尔伯特的思想在当时还蒙上了一层阴影, 那就是对于逻辑理论的不够了解①. 一直到 1917 年至 1918 年, 希尔伯特才又回到建立这个纲领的主题上来. 这时他对逻辑学的了解已经有了改进, 也更加自觉地看到他的计划所包含的可观的技术困难. 其他数学家在促进这种进一步的了解上也起了显著的作用. 到 1921 年左

①他在 1905 年提出的逻辑学, 还落后于弗雷格在 1879 年提出的系统, 或者佩亚诺在 1890 年代提出的系统. 但是我们不来讨论这段时期里逻辑学的发展 (例如可以参看 (Moore, 1998)).

右, 希尔伯特在自己的助手伯奈斯的帮助下, 对于数学的形式化已经有了很精细的概念, 也认识到有必要更深刻更仔细地探索数学证明和数学理论的逻辑结构. 1922年晚些时候, 他第一次在莱比锡的一次讲演里清楚地陈述了自己的纲领.

在这里将要描述希尔伯特纲领的成熟形式, 如他在 1925 年的论文《论无穷》(见论文集 (van Heijenoort, 1967), [也可参看 (Benacerraf P, Putnam H, 1983)]) 中所陈述的那样. 这个纲领的主要目的是利用句法的相容性证明来建立现代数学的原理和推断方式的逻辑可接受性. 公理化、逻辑和形式化使得有可能从纯粹数学的观点来研究数学理论 (所以就叫做**元数学**), 而希尔伯特希望能用非常弱的工具来确立这个理论的相容性. 特别是他希望能回答布劳威尔和外尔的所有的批评, 这样来论证集合理论、经典的实数理论、古典分析, 当然还有古典逻辑, 包括 PEM(这是用归谬法 (reductio ad absurdum) 作间接证明的基础) 在内.

希尔伯特的途径的整个要点在于使数学力量充分精确, 所以可以得到关于其性质的精确的结果. 为了完成这个纲领, 以下的步骤是不可少的:

(i) 找到一个数学理论 T, 例如实数理论的适当的公理和原始概念.

(ii) 找到古典逻辑的公理和推断规则, 使得从已知命题到新命题的过渡是一个纯粹的句法的形式的程序.

(iii) 用形式逻辑演算把 T 形式化, 使得 T 中的命题只不过是一串符号, 而证明则是服从推断的形式规则的符号串序列.

(iv) 在 T 中作一个形式证明, 来表明不可能得出一个表示矛盾的符号串作为一个证明的最后一行, 对这个证明作**有穷的**研究.

事实上, 步骤 (ii) 和 (iii) 对于某些理论, 已经用相当简单的一阶逻辑中形式化的系统解决了, 在任意的数理逻辑的引论中, 例如对戴德金 — 佩亚诺算术或者策墨罗 — 弗朗克尔集合论都已经研究过. 结果是一阶逻辑就已经足够把数学证明编为法典, 有趣的是这个认识来得很晚, 是在*哥德尔定理*[V.15] 得到证明以后.

希尔伯特的主要洞察在于当理论已经形式化以后, 任意的证明都变成了**有限的**组合学的对象, 不过是符合这个系统的形式规则的符号串的阵列. 正如伯奈斯说过的那样, 这只是把理论 T 的演绎结构 "投影" 到数论领域罢了, 而在这个领域中有可能表示出 T 的相容性. 这些认识提高了一种期望, 就是只需对形式化的证明作有穷的研究, 就足以确立理论的相容性, 也就是可能证明那个表示 T 的相容性的那个语句. 但是这种期望并没有得到以前的洞察的保证, 而且证明是错的①.

另外, 这个纲领有一个关键性的前提, 就是不仅是逻辑演算, 还有每一个公理系统都需要是**完全的**. 粗略地说, 所谓完全就是它们要足够强大, 允许导出所有有关的结果②. 哥德尔指出, 这个假设对于包括 (原始递归算术) 的系统是错误的.

---

①更详细的细节例如可见 (Sieg, 1999).

②"有关的结果" 的概念当然要弄确切, 这样做就会引导到句法的完全性或语义的完全性.

还需要对于希尔伯特所谓的**有穷主义**是什么意思说几句话 (详见 (Tait, 1981)). 在好几点上, 1920 年代的希尔伯特纲领在一定程度上采纳了庞加莱和外尔的直觉主义, 而强烈地偏离了希尔伯特本人在 1900 年的思想. 这里正是其中一点. 关键的思想是与弗雷格和戴德金的逻辑主义观点相反, 逻辑和纯粹思维需要一些在我们从直接经验 "直觉地" 得到的东西: 符号和公式.

1905 年, 庞加莱就已经提出一个观点, 算术的相容性的形式证明会是循环论证, 因为这样一个证明必须对公式和证明的长度归纳地进行, 所以就会依赖于它想要证明的归纳法公理. 希尔伯特在 1920 年代对此回应指出, 在元数学层次上所需的归纳法, 比完全算术归纳法要弱得多, 而这种弱的形式是基于对我们直觉接受的符号作有穷考虑得出的. 有穷数学不需要任何进一步的论证或化简.

希尔伯特纲领是先从研究弱的理论开始, 再逐渐地进到较强的理论. 一个形式系统的元理论研究的是诸如相容性、完全性和其他一些性质 ("完全性" 的逻辑意义, 就是所有可以用这个演算来表示的真或者说有效的公式都可以在此系统里导出). 命题逻辑很快就被证明是既相容又完全的. 一阶逻辑或称谓词逻辑是哥德尔在他的 1929 年的学位论文中证明为完全的. 在整个 1920 年代, 希尔伯特以及他的共同工作者的注意力都放在初等算术及其子系统上, 一旦这一点解决了, 就计划转移到更困难也更关键的实数理论和集合理论的场合. 阿克尔曼 (Wilhelm Ackermann, 1896–1962, 德国数学家) 和冯 · 诺依曼已经能够对算术的某些子系统证明相容性, 但是在 1928 年到 1930 年, 希尔伯特深信, 整个算术的相容性已经得到证明. 就在这时, 受到了哥德尔的不完全性定理的沉重打击 (见第 4 节).

用 "形式主义" 这个名称来描述这个纲领, 来自于希尔伯特的**方法**在于把每一个数学理论都形式化, 并形式地研究它的证明的结构. 然而, 这个名称相当片面甚至有些混淆不清, 特别是由于人们常把它与直觉主义对照着来看. 直觉主义确实是一种成熟的数学哲学. [但形式主义不然], 希尔伯特和绝大多数数学家一样, 从来没有把数学看成是用公式来玩的游戏. 说真的, 他时常强调 (非形式的) 数学命题之富有含义, 以及它们的概念的内容的深度[①].

3.3 个人的纠纷

危机不只是在智慧的层面上展开的, 而且也在个人层面上展开. 人们可能会把这个故事当成一场悲剧, 主角的性格和后来的事件造成了很难避免的最终结果.

希尔伯特和布劳威尔是性格非常不同的人, 两人都极为任性而又绝顶聪明. 布劳威尔的世界观是唯心主义的, 而倾向唯我论. 他有艺术家的气质和孤僻的个人生活. 他蔑视现代世界, 寻找自己的内省的生活, 以为这是唯一的出路 (至少在原则上

①例如在 Rowe(1992) 编的讲义里, 以及在他 1930 年同标题的论文 (Gesammelte Abhandlungen, vol 3) 中这是很明显的.

是, 而且做起来也并不如此). 他宁可孤独地工作, 但是在数学界又不乏好友, 特别是在围绕着他的全世界的拓扑学家圈子里. 希尔伯特在观点和态度上都是典型的现代主义者, 充满乐观主义和理性主义. 他想领导他的大学、他的祖国和国际社会走向新世界. 他非常喜欢合作, 而在克莱因关于发展机构和取得权力的计划里如鱼得水.

作为第一次世界大战的后果, 德国人在 1920 年代的早期被禁止参加世界数学家大会. 当 1928 年机会终于来到时, 希尔伯特急于抓住这个机会, 而布劳威尔则非常生气, 因为对德国代表的限制并未取消, 而且发了一封公开信争取以此说服其他数学家. 他们的观点早已是众所周知, 这样造成了两人的冲突. 在另一个层面上, 希尔伯特在 1920 年代就已经向自己的对手作了重要的让步, 希望能在寻求相容性的计划上得到成功. 布劳威尔强调了这些让步, 但是就作者身份问题攻击希尔伯特, 要求希尔伯特作进一步的让步[①]. 希尔伯特可能是感觉自己受到侮辱甚至威胁, 而这些又来自一位他曾经认为是年轻一代中最伟大的数学家.

1928 年发生的事件可能是压断骆驼背的最后一根稻草. 自 1915 年以来, 布劳威尔一直是当时最权威的数学刊物《数学年刊》(*Mathematische Annalen*) 的编委, 而希尔伯特从 1902 年起就是主编. 他厌烦 "有害的贫血症", 同时也看得出希尔伯特觉得自己也快到头了, 担心刊物的未来, 所以他决定, 必须从编委会里除掉布劳威尔. 当他写信给其他编委解释自己的计划时 (实际上已经开始实行这个计划了), 爱因斯坦的回答是, 这个计划不聪明, 拒绝与它发生关系. 但是其他编委显然是不想让德高望重的希尔伯特生气, 最后采取了一个可疑的步骤, 把整个编委会解散, 而成立新编委会. 布劳威尔为此大为烦恼, 结果是这个刊物失去了爱因斯坦和以前曾经是主要编委的卡拉特沃多利 (Constantin Caratéodory, 1873–1950, 出生在德国的希腊数学家)(van Dalen, 2005).

在这以后, 布劳威尔有好几年没有发表文章, 几本书的写作计划也没有完成. 随着他淡出舞台和以前的政治纷争的逐渐平息, "危机" 的感觉也就逐渐消退了 (Hesseling, 2003). 希尔伯特也不再很多地参加以后的辩论和数学基础的发展了.

4. 哥德尔和留下的创伤

希尔伯特不仅是赢得了年刊之战, 数学界整个说来是继续在现代数学的风格下工作. 但是哥德尔的著名的 1931 年的论文在《数学与物理学月刊》(*Monatshefte für Mathematik und Physik*) 上发表, 给了希尔伯特纲领一个沉重而又深刻的打击. 元数学的一个极其聪明的发展 —— 元数学的算术化 —— 使得哥德尔能够证明, 如公理化集合论和戴德金 — 佩亚诺算术这样的系统都是不完全的 (见条目**哥德尔定理**[V.15]). 就是说存在这样的严格地使用该系统的语言来陈述的命题 p, 使得 p 与

①见布劳威尔在 1928 年写的《关于形式主义的直觉主义思考》一文 (Mancosu, 1998).

$\neg p$ 都不能在该系统中形式地证明.

这个定理给希尔伯特的努力提出了一个深刻的问题, 因为它表明了形式证明甚至不能把算术问题都囊括在内. 但是还有更甚者. 详细地看一看哥德尔的论证就清楚了, 这一个元数学的证明本身也可以形式化, 这就引导到了 "哥德尔第二定理", 用上述**系统内**的任意证明都不可能确立这个系统的相容性. 哥德尔的元数学的算术化, 使得可能用形式算术的语言来造出一个句子表示这一个系统的相容性, 但这个句子恰好就在那些不能证明的句子之内①. 换一个角度来讲, 关于 $1=0$ 之不可证明性的一个 (可以在形式算术系统中编写的) 有穷形式证明, 可以变成此系统中的矛盾! 所以, 即令此系统真是相容的 (绝大多数数学家都相信), 其相容性也不会有有穷的证明.

按照哥德尔当时所谓的 "冯 · 诺依曼猜想" (即如果有相容性的有穷证明, 则此证明必可在初等算术内形式化地写出来), 第二定理蕴含了希尔伯特纲领的失败 (见 (Mancosu, 1999, 38) 或者比较好读的 (Dawson, 1997, 68 页以下)). 需要强调的是哥德尔的否定的结果完全是构造性的, 甚至是有穷的, 对于辩论的各方都是有效的. 它们很难消化, 但是到头来, 引导到基础研究的基本事项的重新确立.

由于有根岑类型的证明理论, 以及*模型理论*[Ⅳ.23] 的兴起等, 数理逻辑和基础研究继续光辉地发展, 它们的基础都在 20 世纪前三分之一的基础研究中. 虽然对于今天数学的绝大部分, 策墨罗 — 弗朗克尔的公理系统已经足够给出严格的基础了, 并且利用集合的 "迭代"②概念, 已经有了相当能够服人的直觉的论证, 普遍的感觉是基础研究并没有达到自己雄心勃勃的目标, "而是发现自己已经被卷入数学活动的漩涡里去了, 现在在数学的元老院里面有着完全的选举权 ③".

然而, 这个印象失之于过分表面化. 证明论发展了, 而在把经典理论化为可以认为是构造的系统方面得到了值得注意的化约方法. 一个突出的例子是分析可以在算术的所谓**保守扩张**中形式化. 所谓保守扩张, 就是说, 它是算术的语言的扩张, 其中包括了算术的所有定理; 但又是 "保守的", 就是说它在算术的语言上没有任何新的结果. 分析的有些部分甚至可以在原始递归算术的保守扩张中发展起来 (Feferman, 1998), 这就对相关的构造主义理论的可容许性的哲学基础何在提出了问题. 但是对于这些系统, 问题远不如希尔伯特的有穷数学那么简单. 说迄今还没

①进一步的细节可见 (Smullyan, 2001; Heijenoort, 1967) 和数理逻辑的好的入门书. 这两个定理都在 (Hilbert, Bernays, 1934/39) 中有详细的证明. 关于哥德尔的结果的写得很差的讲述和有毛病的解释更多.

②基本的思想是把集合论的宇宙看成是以下的运算的迭代: 从一个基本的域 V_0(可能是有限的甚至是 $\varnothing$) 开始, 作这个域的元素所成的一切可能的**集合**; 就给出一个新的域 V_1, 然后迭代地构成集合 $V_0 \cup V_1$, 这样做下去 (直至无穷, 甚至超过无穷!) 就构成一个没有头的集合论的宇宙, 这一点在 (策墨罗, 1930) 中非常杰出地描述过. 关于迭代的概念, 可见 (Benacerraf P and Putnam H, 1983) 的最后一篇文章.

③这是 Gian Rota 在 1973 年一篇文章里的话.

有一般的共识, 似乎是公平的.

不论其根源何在, 其存在的正当性的根据何在, 数学总是一种人类的活动. 这种说法的真实性可以从我们的故事后来的发展看得很清楚. 数学社会拒绝放弃 "经典的" 思想和方法; 构造主义的 "革命" 已经流产了. 形式主义虽然有上述的失败, 在实践中仍是 20 世纪数学所承认的意识形态. 有人说, 形式主义并不真是一种信仰, 只不过是有些人一周的六个工作日都把数学对象当作很真实的东西在做, 而到了星期日就 [好像进教堂做礼拜那样] 把形式主义当作一个避难所罢了. 也如一位布尔巴基[VI.96] 的成员说的那样, 什么时候才会放弃工作日里的柏拉图主义? 只有在遇到关于数学知识的不受欢迎的哲学问题, 需要一个现成的答案时才会放弃.

应该注意, 形式主义很适合自觉的自治的做研究工作的数学家社会的需要. 形式主义给他们以选择研究主题的充分自由, 给他们使用现代数学工具去探讨这些主题的充分自由. 但是对于那些惯于反思的数学家, 很久以来就明白, 这不是答案. 关于数学知识的认识论问题, 并没有 "从世界上消除"; 哲学家、历史学家、认知科学家和其他人一直在寻找理解数学的内容与发展的更充分的途径. 不需要说这并没有威胁研究数学的人的自治 —— 如果真关心自治的话, 或许更应该关心市场和其他力量对我们施加的压力.

(半) 构造主义和现代数学二者都在发展, 她们之间的对比简单地就是固化了, 虽然是一种很不平衡的对比, 因为实际在做工作的数学家 99% 是 "现代" 数学家 (但是在涉及什么是数学的正确的方法时, 统计数字又有什么意义呢?), 阿达玛[VI.65] 在评论 1905 年法国的辩论时说过 "显然有两种关于数学的概念, 有两种心理状况". 现在应该认识到, 两种途径各有其价值: 它们是互补的, 可以和平共存. 特别是近几十年来, 对于有效的方法、算法和计算数学的兴趣增长了 —— 这些都更接近于直觉主义的传统.

关于基础的辩论, 在思想和结果上, 在关键的洞察和发展上, 都留下了很丰富的遗产, 包括公理化集合论和直觉主义的兴起. 最重要的发展之一是现代数理逻辑作为公理学的改进的发展, 引导到递归和可计算性理论在 1936 年左右的发展 (见算法[II.4 §3.2]). 在这个过程中, 我们对于形式系统的特征、可能和局限性的理解都大大澄清了.

在整个辩论中, 最热门的主题可能也就是这场辩论最主要的来源, 就是怎样理解连续统的概念. 读者会回忆起对于实数理论的集合论的了解与布劳威尔的途径的对比, 后者拒绝了连续统是由点 "构建" 起来的观点. 由于对康托的连续统假设 (CH) 的结果, 更明确了这是一个迷宫似的问题, 按照这个假设, 实数集合的势 (cardinality) 是第二个超限数 $\aleph_1$, 或者用等价的说法表述即是: $\mathbf{R}$ 的每一个无穷子集合, 或者双射到 $\mathbf{N}$, 或者双射到 $\mathbf{R}$ 自身. 1933 年哥德尔证明了 CH 与公理化集合论是相容的, 而科恩在 1963 年又证明了 CH 与这些公理是独立的 (也就是说, CH

的否定也与公理化集合论[IV.22 §5] 是相容的). 这个问题现在还是活着的问题, 有少数数学家在对连续统提出另外的途径, 另一些人则试图找出新的服人的集合论的原理来解决康托的问题 (Woodin, 2001).

关于基础的辩论, 也以一种确定的方式, 对于澄清现代数学的特殊风格和方法论有贡献, 特别是对于澄清现代数学的柏拉图主义和存在特性有贡献 (见论文集 (Benacerraf, Putnam, 1983) 中所载的伯奈斯的 1935 年的经典论文), 它弄明白了现代数学的柏拉图主义和存在特性, 只是一种 (或至少是一种) 方法论的特性, 而不蕴含任何一种形而上学的存在性. 现代数学是认为它的元素独立于人类 (或机械) 的有效的定义能力和构建能力, 这样来研究数学的结构的. 这可能听起来惊人, 但是, 说不定这个特性可以用科学思想更广泛的特性来解释, 用数学结构在给科学现象建模的作用来解释.

说到头, 这场辩论弄清楚了数学及其现代方法还被重要的哲学问题包围着. 很大一部分的数学知识可以认为是没有问题的, 定理可以得到确立, 问题可以解决, 而且都是确定无疑的、清楚的. 但是凡是想要把它们的本原展示出来, 哲学问题就不可避免. 本文的读者可能已经在好几个地方感觉到这一点, 特别是在关于直觉主义的讨论上感觉到这一点, 但是在希尔伯特纲领后面的基本思想上, 当然也在现实数学与其非形式的对手的关系上, 也会感觉到这一点, 而哥德尔的定理恰好是尖锐地聚焦在这个问题上.

致谢　作者要感谢 Mark van Atten, Jeremy Gray, Paolo Mancosu, José Puiz, Wilfred Sieg 和编者对本文前一稿的有益的评论.

进一步阅读的文献

这里不可能把 Bernays, Brouwer, Cantor, Dedekind. Gödel, Hilbert, Kronecker, von Neumann, Poincaré, Russell, Weyl, Zermelo 等的有关文章都列出来. 读者很容易在下面列出的资料集里面找到 (van Heijenoort, 1967; Benacerraf Putnam, 1983; Heinmann, 1986; Ewald, 1996; Mancosu, 1998).

Benacerraf P and Putnam H, eds. 1983. *Philosophy of Mathematics: Selected Readings.* Cambridge: Cambridge University Press.

Dawsen Jr J W. 1997. *Logical Dilemmas: The Life and Work of Kurt Gödel.* Wellesley, MA: A. K. Peters.

Ewald W, eds. 1996. *From Kant to Hilbert: A Source Book in the Foundations of Mathematics*, 2 vols. Oxford: Oxford University Press.

Feferman S. 1998. *In the Light of Logic.* Oxford: Oxford University Press.

Ferreirós J. 1999. *Labyrinth of Thought: A History of Set Theory and Its Role in Modern Mathematics.* Bassel: Birkhäuser.

Heinzmann G, ed. 1986. *Poincaré, Russell, Zermelo et Peano.* Paris: Vrin.

Hesseling D E. 2003. *Gnomes in the Fog: The Reception of Brouwer's Intuitionism in the 1920's.* Basel: Birkhäuser.

Heyting A. 1956. *Intuitionism: An Introduction.* Amsterdam: North Holland. Third revised edition, 1971.

Hilbert D and Bernays P. 1934/39. *Grundlagen der Mathematik,* 2 vols. Berlin: Springer.

Mancosu P, ed. 1988. *From Hilbert to Brouwer: The Debate on the Foundations of Mathematics in the 1920's.* Oxford: Oxford University Press.

—. 1999. Between Viena and Berlin: The Immediate Reception of Gödel's Incompleteness Theorems. *History and Phiosophy of Logic,* 20: 33-45.

Mehrtens H. 1990. *Moderne-Sprache-Mathematik.* Frankfurt: Suhrkamp.

Moore G H. 1982. *Zermelo's Axiom of Choice.* New York: Springer.

—. 1998. Logic early twentieth century. In *Routledge Encyclopedia of Philosophy,* edited by Craig E. London: Routledge.

Rowe D. 1992. *Natur und mathematisches Erkennen.* Basel: Birkhäuser.

Sieg W. 1999. Hilbert's programs: 1917-1922. *The Bulletin of Symbolic Logic,* 5: 1-44.

Smullyan R. 2001. *Gödel's Incompleteness Theorems.* Oxford: Oxford University Press.

Tait W W. 1981. Finitism. *Journal of Philosophy,* 78: 524-46.

Van Atten M. 2003. *On Brouwer.* Bermont, CA: Wadsworth.

Van Dalen D. 1999/2005. *Mystic, Geometer, and Intuitionist: The Life of L. E. J. Brouwer.* Volume Ⅰ: *The Dawning Revolution.* Volume Ⅱ: *Hope and Disillusion.* Oxford: Oxford University Press.

Van Heijenoort J, ed. 1967. *From Frege to Gödel: A Source Book in mathematical Logic.* Cambridge: Cambridge University Press(Reprinted, 2002).

Weyl H. 1918. *Das Kontinuum.* Leipzig: Veit.

Whitehead N R and Rssell B. 1910/13. *Principia Mathematica.* Cambridge: Cambridge University Press. Second edition, 1925/27, (Reorinted, 1978).

Woodin W H. 2001. The continuum hypothesis, Ⅰ, Ⅱ. *Notices of the American Mathematical Society,* 48: 567-576, 681-690.

第III部分　数学概念

III.1　选择公理 (The Axiom of Choice①)

考虑以下问题：容易找到两个无理数 a，b 使 $a+b$ 为有理数，或者使 ab 为有理数 (在这两个情况都可以取 $a=\sqrt{2}$，$b=-\sqrt{2}$)，但是能否使得 a^b 也是有理数？是的. 下面是一个优美的回答. 令 $x=\sqrt{2}^{\sqrt{2}}$. 如果 x 已是一个有理数，则得到所需的例子 [$a=b=\sqrt{2}$ 就可以了；但是，如果 x 不是有理数，而是无理数，则令 $a=x=\sqrt{2}^{\sqrt{2}}$，而 $b=\sqrt{2}$，则 $a^b=x^{\sqrt{2}}=\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}}=(\sqrt{2})^{\sqrt{2}\cdot\sqrt{2}}=(\sqrt{2})^2=2$，就又得到了一个例子].

现在的这个论证肯定已经确定了有这样的可能，即 a 和 b 都是无理数，而 a^b 是有理数. 然而这个证明有一个非常有趣的特点：它是**非构造性的**，就是说，它并没有明确指出哪两个无理数能行. 相反，它告诉我们或者令 $a=b=\sqrt{2}$，或者令 $a=\sqrt{2}^{\sqrt{2}}$，$b=\sqrt{2}$，总有一个情况能行. 它不仅没有告诉我们起作用的究竟是哪一种情况，甚至一点线索都没有给我们②.

这样一种论证一直让哲学家和倾向于哲学的数学家烦心，但是就主流的数学而言，它是一个完全被接受的重要类型的推理方法. 形式地说，我们是求助于"排中律". 我们已经证明了某个命题的否定不可能为真，由此导出这个命题本身必定为真. 对于以上证明的典型反应，并不是说它在哪种意义下不行，而是它的非构造本性让人惊奇.

然而，面对着这样一个非构造的证明，很自然地会去问，能否找到构造性的证明. 说到底，一个实实在在的构造会使我们对这个命题有更多的洞察. 这一点很重要，因为我们去证明一件事情，不仅是为了确知它为真，而想对于它**为什么**为真有一点概念. 当然，要找一个构造性证明并不是因为非构造性的证明不对，而只是有一个构造性的证明可以提供更多信息.

选择公理是从一些集合做出其他集合的几个规则之一. 这种规则的两个典型例子是下面的命题：对于任意的集合 A，可以作出其一切子集合的集合，[称为 A 的幂

① 这一部分的条目是按字母顺序排列的，所以我们把各个条目的英文标题附上. —— 中译本注

② 但是在本书 [III.42] 中指出了由 Gelfond-Schneider 定理，$\sqrt{2}^{\sqrt{2}}$ 是一个超越数. —— 中译本注

集], 还有对于任意的集合 A 和任意的性质 p, 可以作出 A 中的所有具有性质 p 的元素的集合 (这两条规则分别叫做**幂集公理**和**概括公理**). 粗略地说, 选择公理说的就是允许我们在作出一个新集合的时候作任意多次未加特别说明的选择.

和其他公理一样, 选择公理可能看起来是那么自然, 以至于我们在使用它的时候还不觉得正在用它, 真正的情况也是, 在它第一次被形式地陈述以前, 许多数学家都用过它了. 为了对于它说的是什么有所了解, 我们来看一下大家知道的可数集合的可数族之并仍是可数集合[III.11] 的证明. 这个族为可数的事实, 使我们能把它们列成一个单子 $A_1, A_2, A_3, \cdots$, 然后, 每一个单个的集合 A_n 也可数这一事实, 又使我们能把它的元素列成一个单子 $a_{n1}, a_{n2}, a_{n3}, \cdots$. 最后, 找一个系统的方法把所有的元素 a_{nm} 都数遍, 就完成了证明.

在这个证明里面, 我们确实做了无数次未经特别说明的选择. 我们被告知, 每个 A_n 都是可数的, 然后就对 A_n 的元素 "选择" 了一个单子, 而**未特别说明**是怎么选的. 进一步, 因为绝对没有对我们说明过这些 A_n, 所以当然也不可能说明是怎样把它们排列成一个单子的. 这一点并没有使证明失效, 但是它确实说明这个证明是非构造性的 (注意, 如果确实告诉了我们这些集合 A_n 究竟是什么, 就很可能说明怎样把它的元素列成单子, 这样就对这些集合之并为可数集合得出一个构造性的证明).

下面是另一个例子. 如果可以把一个图[III.34] 的顶点分成两类 X 和 Y, 使得同一类的任意两个顶点都不能用这个图的一个边连接起来, 我们就说这个图是**二分的**(bipartite) . 例如一个偶循环 (就是排在一个圆周上的偶数个点, 而把相邻的点连接起来) 就是二分的, 而没有一个奇循环是二分的. 那么, 无数多个偶循环的不相交并集合是不是二分的? 当然是的: 把每一个循环 C 的顶点分成两类 X_C 和 Y_C, 然后令所有 X_C 之并为 X , 所有 Y_C 之并为 Y , 这样就行了. 但是对每一个 C, 我们选哪一个称为 X_C, 哪一个称为 Y_C 呢? 我们不能具体地说明这一点, 所以, 我们又是应用了选择公理 (只不过没有说罢了).

一般说来, 选择公理宣称: 若给定一族非空集合 X_i, 则从每一个 X_i 中, 可以选择一个元素 x_i. 更准确地说, 它宣称: 若 X_i 为非空集合, 而 i 是一个指标集合 I 的元, 则有一个定义在 I 上的函数 f, 使对所有的 i , $f(i) \in X_i$. 这个函数称为这个族的**选择函数**.

对于一个集合, 我们用不着任何单个的规则来做这件事. 事实上, 一个集合 X_1 为非空这个命题, 就是 [一个关于选择的] 命题: 存在 $x_1 \in X_1$(更形式的说法是: 映 1 为 x_1 的函数, 就是这个仅含一个 X_1 的集合之 "族" 的选择函数). 对于两个集合, 其实对于任意有限多个集合的族, 我们都可以用对于集合个数作归纳来证明选择函数的存在. 但是对于无限多的集合, 不能从其他的构造集合的规则来证明选择函数的存在.

为什么要对选择公理大惊小怪呢? 主要的理由在于, 如果在某个证明中应用了

选择公理, 则证明的那一部分就自动地是非构造的了. 这一点也就会反映在命题本身. 对于我们所用的其他规则, 例如 “我们可以取两个集合之并”, 则断定其存在的那个集合是由它的性质唯一地确定的 (u 是 $X \cup Y$ 的元素, 当且仅当它是 X 或 Y 的元素, 或同时是二者的元素). 但是对于选择公理就不是这样, 断定其存在的对象 (选择函数) 并不是由它的性质唯一地指定的, 在典型情况下, 都有许多选择函数存在.

由于这个原因, 主流数学的一般观点是, 哪怕选择公理用得没有问题, 最好还是指明是应用了它, 以便提请注意, 这个证明是非构造性的.

一个其证明用到了选择公理的例子是*巴拿赫–塔斯基悖论*[V.3]. 这个悖论说有一种方法把一个单位球体分成有限多子集合, 然后 (用旋转、反射和平移) 把这些子集合重新合并起来成为两个单位球体. 证明并未给出如何定义这些子集合.

人们有时说, 应用选择公理 “令人不快”, 或者说它的结果是 “高度违反直观的”, 但是在绝大多数情况下, 稍想一想就会发现, 这些结果并没有违反直观. 例如再考虑一下上述的巴拿赫–塔斯基悖论. 为什么它看起来很奇怪, 似乎是悖论? 这是因为我们觉得体积没有保持不变. 而事实上可以把这种感觉转变为严格的论据, 即这个分解所形成的子集合不可能都是可以有意义地赋予体积的那种集合. 但是这根本不是悖论, 对于一个好的集合, 例如多面体, 我们可以说清楚所谓体积是什么意思, 但是完全没有理由假设对于球体的**所有**子集合, 我们都能够有意义地定义其体积 (有一个数学分支叫做测度论, 可以用来给很大一类子集合, 即*可测集*[III.55], 赋以体积, 但是完全没有理由相信所有的集合都是可测集, 而且可以证明确实有不可测的集合存在, 不过这里又要用到选择公理).

选择公理在日常的数学生活里比上述的基本形式用得更多的还有两个形式. 其一是**良序原理**, 它宣称所有的集合都可以*良序*[III.66]. 另一个是佐恩 (Max August Zorn, 1906–1993, 出生于德国的美籍数学家)**引理**, 它指出, 在一定条件下必有 “最大” 元素存在. 例如, 一个向量空间的基底就是最大的线性无关集合, 而结果是, 若对向量空间的线性无关集合的整体应用佐恩引理, 就可以证明每一个向量空间都有基底存在.

这两个命题都被说成是选择公理的形式, 是因为它们都等价于选择公理, 就是说, 在其他的构造集合的规则都存在的条件下, 它们的每一个都蕴含着选择公理, 也可以从选择公理导出. 要想看出为什么选择公理的这两个形式都有一种非构造的感觉, 一个好办法是花上几分钟想一想怎样找出实数集合的良序, 或者找出有所有实数序列所成的向量空间的基底.

关于选择公理, 特别是关于它与形式集合理论的其他公理的关系, 可以参看条目*集合理论*[IV.22].

III.2 决定性公理

(The Axiom of Determinacy)

考虑以下的 “无限博弈”. 有两个局中人 A 和 B, 依次各给出一个自然数, 例如设 A 为先手. 这样, 他们就会作出一个自然数的无限序列. 如果这个序列是 “最终周期的”, 则 A 胜, 否则 B 胜 (一个最终周期序列就是像 1, 56, 4, 5, 8, 3, 5, 8, 3, 5, 8, 3, 5, 8, 3, $\cdots$ 这样的序列, 经过一定步数以后就会停留在一个反复的模式上, [就像循环小数那样]). 不难看到, B 有一个致胜策略, 因为最终周期序列是很特殊的. 然而, 在博弈的任意阶段, A 仍然可以制胜 (只要 B 玩得足够糟糕), 因为每一个有限序列都是许多最终周期序列的开始的一段.

更一般地说, 自然数的无限序列的任意集合 S 都会给出一个无限博弈: A 的目标是使得所得的序列是 S 的一个元素, B 的目标则相反. 如果两个局中人之一有一个制胜策略, 就说这个博弈是**决定性的**. 我们已经看到, 如果 S 是所有最终周期序列的集合, 这个博弈一定是决定性的, 而实际上, 对于我们不论怎样来写出的 S, 相应的博弈也一定是决定性的. 但是结果是确有不是决定性的博弈存在 (有一个很有教益的练习, 看一看下面的似乎正确的论据错在哪里: “如果 A 没有制胜策略, 就不能一定得胜, 所以 B 一定有制胜策略”).

不难作出非决定性的博弈, 但是构造这个博弈要用到选择公理[III.1] 如下: 粗略地说, 可以把所有可能的策略的集合良序化 ([良序原理是等价于选择公理的]), 所以每一个前面的策略即前置元 (predecessor) 的个数总少于无限序列的个数, 把这样的序列放进 S 或其余集, 就使得每一个策略都不能成为任一个局中人的制胜策略, **决定性公理**宣称, 每一个博弈都是决定性的. 它与选择公理矛盾, 但是如果把它加进**没有**选择公理的策墨罗–弗朗克尔公理系统[III.99], 它就是一个很有趣的公理. 例如, 它事实上蕴含了许多实数集合具有惊人的好性质, 例如所有的实数集合都是勒贝格可测集合. 决定性公理与大基数理论有密切关系, 详见条目集合理论[III.22].

巴拿赫空间

(Banach Spaces)

见赋范空间与巴拿赫空间 [III. 62]

III.3 贝叶斯分析

(Bayesian Analysis)

如果掷出两颗标准的骰子, 掷出总数为 10 的概率是 $\frac{1}{12}$, 因为掷出的结果共有

36 种, 而其中只有 3 种总和为 10(即 4 与 6, 5 与 5, 6 与 4). 但是, 如果第一颗骰子投出为 6, 则在知道了这个信息的条件下, 掷出的总和仍为 10 的**条件概率**就是 $\frac{1}{6}$(这就是另一颗骰子掷出 4 点的概率).

一般说来, **在条件 B 下出现 A 的概率**定义为 A 与 B 同时出现的概率再除以 B 出现的概率. 用记号表示为

$$P[A|B]=\frac{P[A\wedge B]}{P[B]}.$$

由此可得 $P[A\wedge B]=P[A|B]P[B]$. 但是 $P[A|B]=P[B|A]$, 所以

$$P[A|B]P[B]=P[B|A]P[A].$$

因为左方为 $P[A\wedge B]$ 而右方为 $P[B\wedge A]$. 用 $P[B]$ 通除上式双方, 即得**贝叶斯定理**:

$$P[A|B]=\frac{P[B|A]P[A]}{P[B]}$$

(贝叶斯 (Thomas Bayes), 1702 –1761, 英国数学家), 把条件 B 下 A 的条件概率与条件 A 下 B 的条件概率联系了起来.

统计学的基本问题是分析在一个未知的*概率分布*[III.71] 下得到的数据. 在这里, 贝叶斯定理可以做出显著的贡献. 例如, 已知投掷一些无偏差的硬币, 有 3 个是正面向上. 又设已知硬币的总数在 1 到 10 之间, 请猜一下硬币的数目. 令 H_3 表示 3 个硬币正面向上这个事件, C 表示硬币的数目. 对于从 1 到 10 的 n, 计算条件概率 $P[H_3|C=n]$ 并不难, 但是我们想要知道的是反面的 $P[C=n|H_3]$. 贝叶斯定理告诉我们, 它是

$$P[H_3|C=n]\,\frac{P[C=n]}{P[H_3]}.$$

这个式子告诉我们, 如果知道了 [对于不同的 n], 概率 $P[C=n]$ 是多少, 那么也就知道了各个条件概率 $P[C=n|H_3]$ 之比. 在典型情况下, 我们并**不知道**概率 $P[C=n]$ 是多少, 但是可以作一些猜测, 称为**先验分布**(prior distribution). 例如, 在知道有 3 个硬币是正面向上以前, 我们就可以猜想, 对于从 1 到 10 的每一个 n, 恰好取 n 个硬币来投掷的概率是 $\frac{1}{10}$. 在有了这样的信息以后, 就可以用上面的公式来修正我们的估计, 而得到后验分布, 其中 $C=n$ 的概率将会正比于 $\frac{1}{10}P[H_3|C=n]$.

贝叶斯分析的意义超出了简单地只是用后验分布来代替先验分布. 特别是如上面的例子所指出的, 并不总有明显的先验分布让我们来取, 设计一种选择先验分布的方法, 使它在不同意义下是 “最优的”, 这是一个微妙而有趣的数学问题. 进一步的讨论, 可见条目*数学与医学统计*[VII.11] 与*数理统计学*[VII.10].

III.4 辫 群
(Braid Groups)

F. E. A. Johnson

取两个平行的平面, 每一个各钻 n 个孔, 依次将它们编号为 1 到 n . 然后牵一根绳子, 从一个平面上的一个孔牵到另一平面的一个孔, 但不能让两根绳子穿过同一个孔, 这样就得到一个 n 辫. [把这两个平面竖立起来, 从侧面看过去], 就得到它们的 2 维投影, 而两个 3 辫的 2 维投影就与纽结图示 [III.44] 相似, 可见图 1.

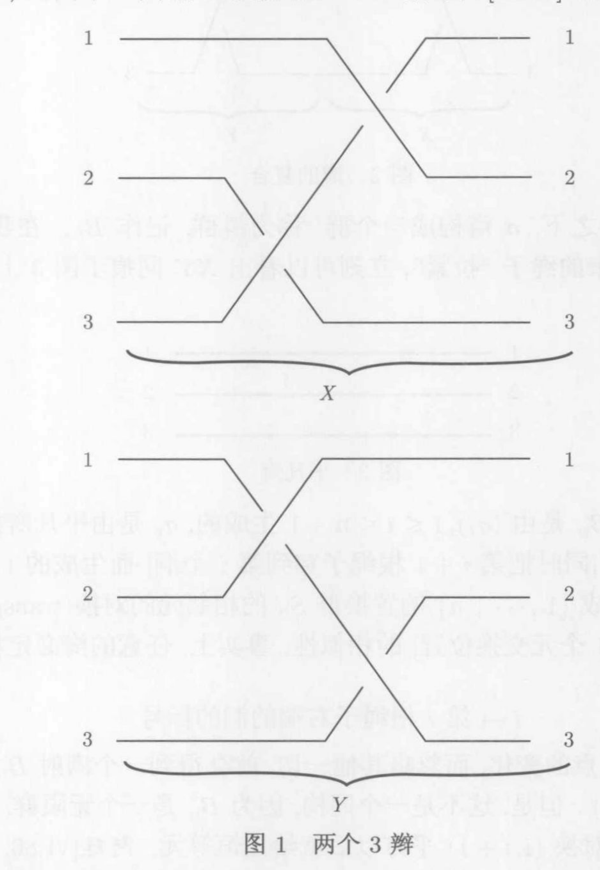


图 1 两个 3 辫

这个图示暗示了我们坚持把绳子从左穿到右, 而且不许 "折转", 所以, 打结的绳子是不许可的.

在此, 在辫的描述上有一定的自由: 只要把绳子的端点固定, 不能拉断绳子, 也不准它们互相穿过, 除此以外, 可以拉伸、压缩、弯曲或者在 3 维空间里移动, 得到的

都算是同样的辫. 这种 “相同性” 是一个等价关系[I.2 §2.3], 称为**辫的同痕**(isotopy).

辫可以组合如下：把两个辫放在一起, 使同编号的孔毗邻地位于一个公共 (居中) 的平面上, 把 [穿过居中平面的同一个孔的] 两根绳子连接起来, 再把居中的平面抽走. 图 2 画的就是图 1 的两个辫 X 与 Y 的复合, 记为 XY .

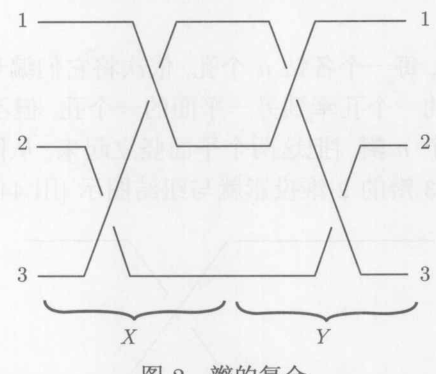


图 2　辫的复合

在这样的复合之下, n 辫构成一个群, 称为辫群, 记作 B_n. 在我们的例子中, $Y=X^{-1}$, 把连起来的绳子 “拉紧”, 立刻可以看出 XY 同痕于图 3 上的**平凡辫**, 其作用就是恒等元.

1　　1
2　　2
3　　3

图 3　平凡辫

作为一个群, B_n 是由 $(\sigma_i), 1\leqslant i\leqslant n-1$ 生成的, σ_i 是由平凡辫把第 i 根绳子穿到第 $i+1$ 个洞 [同时把第 $i+1$ 根绳子穿到第 i 个洞] 而生成的 (见图 4). 读者可以看到, σ_i 与生成 $\{1,\cdots,n\}$ 的置换群 S_n 的相邻元的**对换**(transposition)[即将第 i 个元与第 $i+1$ 个元交换位置] 的相似性. 事实上, 任意的辫必定按照以下的规则决定一个置换：

$$i\mapsto \text{第 } i \text{ 根绳子右端的洞的标号}$$

如果只关注绳子端点的变化, 而忽略其他一切, 就会得到一个满射 $B_n\to S_n$, 把 σ_i 映为对换 $(i\,,\,i+1)$. 但是, 这不是一个同构, 因为 B_n 是一个无限群, 事实上, σ_i 的阶数就是无穷, 而对换 $(i,i+1)$ 平方以后就给出恒等元. 阿廷[VI.86] 在 1925 年的著名论文《辫的理论》(*Theorieder Zöpfe*) 中就证明了, B_n 中的乘法完全由以下关系决定：

$$\sigma_i\sigma_j=\sigma_j\sigma_i\,,\quad |i-j|\geqslant 2\,,$$

$$\sigma_i\sigma_{i+1}\sigma_i=\sigma_{i+1}\sigma_i\sigma_{i+1}\,.$$

这些关系后来发现在统计物理中很重要, 称为 Yang-Baxter 方程式.

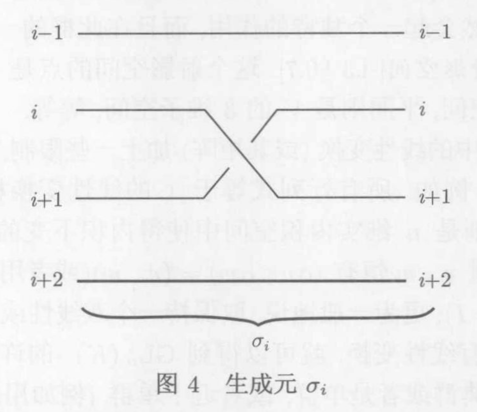


图 4 生成元 σ_i

在由生成元和关系所定义的群中, 要决定生成元的任意的字 (word)[①]是否为恒等元一般是很困难的事. 没有一个在各个情况下都一致可用的方法 (见**几何和组合群论**[IV.10]). 对于 B_n, 阿廷用 "梳辫子" 的方法几何地解决了这个问题. 另一种由 Garside(1967) 提出的代数方法决定了 B_n 的两个元何时为共轭的问题.

关于这些问题是否可判定, 以及在许多其他方面, 辫群都展现了和线性群有密切的亲和关系 (线性群就是所有元素的性态都类似于可逆的 $N \times N$ 矩阵的群). 虽然这种相似性暗示了应该可以证明辫群其实就是线性群. 但是这个问题多年一直没有解决, 直到 2001 年才由 Bigelow 给出了证明, Krammer 也独立地得到了证明.

这里描述的群, 严格地说只是平面上的辫群, 打孔的对象是平面. 其他的辫群还出现在别的地方, 而且时常令人大吃一惊. 它与统计物理的联系上面已经提到了, 它们也在代数几何里出现: 代数曲线去掉例外点, 就是打了孔. 这样, 虽然辫的来源在拓扑学, 却在其他领域里也引人注目地插上一手, 例如在初看起来纯粹是代数问题的 "构造伽罗瓦理论" 中.

III.5 厦
(Buildings)

Mark Ronan

向量空间上的可逆线性变换构成一个群, 称为**一般线性群**. 若向量空间的维数为 n, 标量域为 K, 则此群记为 $\mathrm{GL}_n(K)$. 如果取此向量空间的一个基底, 则此群的每一个元素都可以写成一个 $n \times n$ 矩阵, 而且其**行列式**[III.15] 非零. 这个群及其

① 设 S 为一个群, $s_1, s_2, \cdots, s_m$ 是一些生成元, 则表达式 $s_{i_1}^{r_1} s_{i_2}^{r_2} \cdots s_{in}^{r_n}$ (r_i 为整数) 就称为它们生成的 "字". —— 中译本注

子群在数学中有很大的兴趣, 而且可以对它 "几何地" 进行研究: 不考虑一个向量空间 V, 其中原点自然会起一个独特的作用, 而且在此群的一切变换下都不变, 现在来看与 V 相关的射影空间[I.3 §6.7], 这个射影空间的点是 V 的 1 维子空间, 其直线是 V 的 2 维子空间, 平面则是 V 的 3 维子空间, 等等.

如果对 $\mathrm{GL}_n(K)$ 中的线性变换 (或其矩阵) 加上一些限制, 就可以得到 $\mathrm{GL}_n(K)$ 的一些重要的子群. 例如, 所有行列式等于 1 的线性变换构成特殊线性变换群 $\mathrm{SL}_n(K)$. 群 $O(n)$ 则是 n 维实内积空间中使得内积不变的线性变换 α 所成的群, 即对任意两个向量 v , w 恒有 $(\alpha v, \alpha w) = (v, w)$(或者用 α 的矩阵 A 来表示, 这个条件成为 $AA^{\mathrm{T}} = I$); 更为一般地说, 取保持一个双线性或半线性形式 (sesquilinear form) 不变的所有线性变换, 就可以得到 $\mathrm{GL}_n(K)$ 的许多类似的子群. 这些子群称为**经典群**. 经典群或者是单群, 或者近于单群 (例如用适当的标量矩阵所成的子群求商就可以得到单群). 若 K 是实数域或复数域, 则经典群成为**李群**.

在条目李的理论[III.48] 中讨论了李群及其分类, 简单李群中包括了经典群, 它们包括了四个族 A_n , B_n , C_n 和 D_n, 此外还有 [几个例外的个例]E_6 , E_7 , E_8 , F_4 和 G_2. 下标与群的维数有关, 例如 A_n 型的群就是 $n+1$ 维的可逆线性变换的群.

这些简单李群在任意域上都有类比物, 称为**李型的群**. 例如 K 可以是有限域, 这时群就成了有限群. 可以证明几乎所有的有限单群都是李型的, 见有限单群的分类[V.7]. 在 20 世纪的前半叶, 发展了经典群下面的几何理论. 这个理论使用了射影空间和它的各个子几何学, 这就使得有可能对于经典群给出其类似物, 但是它不能给出 E_6 , E_7 , E_8 , F_4 和 G_2 的类似物. 由于这个理由, 雅克 · 蒂茨①寻求包含所有这些族 [例外情况也在内] 的几何理论, 于是创造了**厦理论**.

一个厦的完全的抽象的定义有点复杂, 所以我们限于只看一下与 A_{n-1} 型的群 $\mathrm{GL}_n(K)$ 和 $\mathrm{SL}_n(K)$ 相关的厦, 以便得到一点了解. 这个厦是一个**抽象的单纯复形**, 而可以看作图[III.34] 的高维类比. 一个厦中包含了一族点, 称为**顶点**; 和在图中一样, 取一些点对, 称为**棱**; 然后就与图不同了, 还可以取一些点的三元组, 构成 2 维的**面**, 仿此以往, 取一些 $k-1$ 维的单形 (simplex) 的集合 ($k-1$ 维单形是由 k 个顶点构成的, 其几何意义就是 k 个处于一般位置的点的凸包, [这里所谓一般位置, 就是要防止出现例如共线这样的特殊情况, 也就是要求它们线性无关], 例如一个非退化的四面体就是一个 3 维单形). 单形的面也要包括在单形之内, 所以 3 个顶点若非每两个顶点都有棱连接, 就不能构成单形.

为了构成 A_{n-1} 型的厦, 先取所有的 1 维、2 维、3 维等各个维数的子空间 (它们在射影空间里分别代表点、线、面等), 把这些子空间当作 "顶点", 然后再作各维

①雅克 · 蒂茨 (Jacques Tits), 1930 年生于比利时, 后入法国籍. 由于公认为开创了群的现代理论, 与美国数学家汤普森 (John Griggs Thompson) 共同得到 2008 年的阿贝尔奖. 厦理论就是他的得奖之作. —— 中译本注

的单形如下：一串依次包含的真子空间就是单形, 例如先有一个 2 维空间, 它含于某个 4 维空间内, 而这个 4 维空间又含于一个 5 维空间内, 这样的 3 个"顶点"就构成一个三角形, 即 2 维单形, 这里的 2 维、4 维、5 维子空间就是它的 3 个顶点. 最大维的单形有 $n-1$ 个顶点, 成为一串套在一起：一个 1 维子空间, 位于一个 2 维子空间之内, 再位于一个 3 维子空间之内, 如此等等. 这些单形就叫做**房**(chambers).

由于子空间为数巨大, 所以一个厦是一个非常巨大的对象. 然而, 厦有重要的子几何对象, 称为**公寓**(apartment), 在 A_{n-1} 的情况, 公寓是这样造出来的：取向量空间的一个基底, 然后取这个基底的一切子集合及其生成的子空间. 例如在 A_3 的情况下, 向量空间是 4 维的, 所以基底由 4 个元素构成, 基底的子集合一共可以构成 4 个 1 维空间、6 个 2 维空间和 4 个 3 维空间. 为了使得这个公寓成为可视的, 一个有用的方法是把这 4 个 1 维子空间看成一个四面体的 4 个顶点, 6 个 2 维子空间看成其 6 个棱的中点, 4 个 3 维子空间看成其 4 个面的重心. [于是, 一个房就由一个顶点、一个连接此顶点的棱 —— 用其中点表示 —— 和挨着这个棱的面 —— 用其重心来表示, 这样就成了一个小三角形]. 这样, 一个公寓就有 24 个房, 每一个面 [分成了 6 个小三角形] 就是 6 个房, 这 24 个房构成了这个四面体表面的一个铺砖结构 (tiling). 这个表面拓扑地等价于球面, 作为这个厦的所有的公寓. 所以, 这个厦就叫做球面厦. 所有李型的群的厦都是球面厦, 而且正如 A_3 的厦与四面体相关一样, 其他的公寓相关于 n 维的正多面体和半正多面体①, 这里 n 就是前面说过的李的记号的下标.

厦有以下两个值得注意的特点. 首先, 任意两个房都位于共同的公寓内. 在上面的例子中这并不显然, 但是可以用线性代数来证明. 第二, 在任意厦中, 所有的公寓都是同构的, 而且任意两个公寓都很漂亮地相交. 所谓漂亮, 准确地说就是如果 A 和 A' 是两个公寓, 则 $A\cap A'$ 为凸, 而且存在一个由 A 到 A' 的同构, 使 $A\cap A'$ 在此同构下不变. 蒂茨原来就是用这两个特点来定义厦的.

球面厦的理论并不只是对李型的群给出了令人愉快的几何基础, 它也可以用于对任意域 K 来构造 E_6 , E_7 , E_8 和 F_4 的厦, 而不需要用李代数这样精巧的工具. 一旦把这些厦构造出来 (而且是用惊人简单的方法来构造), 蒂茨关于自同构存在的一个定理就证明了群本身的存在.

在球面厦里, 公寓就是球面的一个铺砖结构, 但是其他类型的厦也起显著的作用. 特别重要的是**仿射厦**, 这时, 公寓是欧几里得空间的铺砖结构, 这种厦自然地在 $GL_n(K)$ 这样的群中产生, 这里 K 是一个 p 进域[III.51]. 对于这种域, 有两种厦, 一是球面厦, 一是仿射厦, 但是仿射厦带有更多的信息, 而把球面厦给出为"无穷远

①半正多面体是这样的多面体：它的面可以有几种不同类的多边形, 但是同样边数的多边形一定要是恒等的. 例如一个很常见的足球, 就可以是由若干个正 6 边形和若干个正 5 边形组成. 阿基米德发现了半正多面体共有 13 种, 所以半正多面体也叫阿基米德多面体. —— 中译本注

处" 的结构. 再超越仿射厦, 还有双曲厦, 它的公寓是双曲空间的铺砖结构, 它们在研究双曲 Kac-Moody 群时自然地产生.

III.6 Calabi-Yau 流形 (Calabi-Yau Manifold)

Eric Zaslow

1. 基本定义

Calabi-Yau 流形, 以卡拉比 (Eugenio Calabi, 1923–, 意大利裔美国数学家) 和丘成桐 (1949–, Yau Shingtung) 命名, 是从黎曼几何和代数几何中产生的, 在弦论和镜面对称理论中起了显著的作用.

为了解释 Calabi-Yau 流形究竟是什么, 我们先回忆一下**实流形** [I.3 §6.9] 上定向的概念. 如果在一个实流形上可以取局部坐标系, 而且在两个坐标邻域相交的部分上, 两个局部坐标 $x=(x^1,\cdots,x^m)$ 和 $y=(y^1,\cdots,y^m)$ 间有正的雅可比行列式 $\det\left(\partial y^i/\partial x^j\right)>0$, 就说这个流形是**可定向的**. Calabi-Yau 流形就是这种可定向流形的自然的复类比. 现在这个流形是复的, 而对每一个局部坐标系 $z=(z^1,\cdots,z^n)$, 都有**全纯函数**①[I.3 §5.6]$f(z)$. 至关重要的是 f 处处不为零的情况, [这时, 就说这个复流形是 Calabi-Yau 流形]. 这里也有一个相容性条件: 若 $\tilde{z}(z)$ 是另一个局部坐标系, 则相应的全纯 n 形式 $\tilde{f}$ 与 f 之间应有方程式 $f=\tilde{f}\det\left(\partial\tilde{z}^a/\partial z^b\right)$. 注意, 如果把这个定义里的复的名词都换成相应的实的名词, 就得到了实的可定向流形. 所以非形式地说, Calabi-Yau 流形可以设想为具有复定向的复流形.

2. 复流形与厄尔米特结构

在往下讲之前, 先略讲一点复几何和凯勒 (Erich Kähler, 1906–2000, 德国数学家) 几何是合适的. 一个复流形就是一个局部看起来像是 $\mathbf{C}^n$ 的结构. 具体说来, 就是在其每一点都可以找到复坐标 $z=(z^1,\cdots,z^n)$, 而在两个局部坐标 z 和 $\tilde{z}$ 的坐标邻域相交处 $\tilde{z}^a$ 是 z^b 的全纯函数. 这样, 复流形上的全纯函数的概念是有意义的, 而且与坐标的选择无关. 这样, 复流形的局部几何确实就像是 $\mathbf{C}^n$ 的开集合, 而其在一点处的切空间就和整个 $\mathbf{C}^n$ 一样.

在复向量空间上考虑由**厄尔米特矩阵**[III.50 §3]$g_{a\bar{b}}$ 定义的**厄尔米特内积**[III.37] 是很自然的, 这里取 e_a 为基底. 在复流形上, 切空间上的厄尔米特内积称为一个

①更准确地应该说是全纯 n 形式, 下同. —— 中译本注

"厄尔米特度量", 而在一个坐标基底下由依赖于位置的厄尔米特矩阵 $g_{a\bar{b}}$[①]来表示.

3. 黎曼几何的完整性和 Calabi-Yau 流形

在黎曼流形上, 可以把一个向量沿一路径移动, 而且使它保持长度为常值并且"指向相同的方向". 曲率就表示这样一件事实: 一个向量到了路径的终点时会偏离自己 [原来的方向] 而绕过一定大小的角度. 如果这个路径是一个闭环, 这个向量回到路径起点时会成为一个新的向量 (一个好例子是考虑球面上闭的路径: 从北极出发, [沿一经线] 走到赤道, [再沿赤道] 走 1/4 个赤道, [最后再沿一条经线] 回到北极. 当旅行完成时, 一个出发时指向南方的 "常值" 向量, 在再次回到北极时, 将会旋转过 90°). 对于每一个闭环, 都会得到一个 "**完整矩阵**" (holonomy matrix), 把起始的向量变成终结的向量. 这些矩阵所成的群称为这个流形的**完整群**. 因为在这个过程中, 向量的长度未变, 所以完整群应该在保持长度的矩阵的群 —— 正交群 $O(m)$ 内, [这里 m 是这个黎曼流形的维数]. 如果这个流形是可定向的, 完整群必在 $\mathrm{SO}(m)$ 中, 这只要通过移动有定向的基底向量就可以看出来.

每一个复维数为 n 的复流形同时也是实维数为 $m=2n$ 的实流形, 而且可以认为它以原来的复坐标 z^j 的实部和虚部为其实坐标. 例如, 复坐标方向可以乘以 $\mathrm{i}=\sqrt{-1}$ 这件事实蕴含了在 [这样得出的实流形] 的实的切空间上必存在一个算子, 其平方为 -1. 这个算子的本征值为 $\pm\mathrm{i}$, 可以认为它们分别代表 "全纯方向" 和 "反全纯方向". 厄尔米特性质表明, 这两个方向是正交的. 如果在绕过闭环一周后, 它们仍然正交, 就说这个流形是**凯勒流形**. 这意味着其完整群是酉群 $U(n)$ 的子群 (这个酉群本身也就是 $\mathrm{SO}(2m)$ 的子群, 就是说, 复流形总是有实定向的). 凯勒性质有一个很优美的局部的刻画方法: 若 $g_{a\bar{b}}$ 是厄尔米特度量在一个坐标邻域中的分量, 则在此邻域中存在一个函数 φ 使得 $g_{a\bar{b}}=\partial^2\varphi/\partial z^a\partial\bar{z}^b$.

给出一个复定向 —— 就是上面讲的 Calabi-Yau 流形的不用度量的定义 —— 一个相容的凯勒结构会导致其完整群在 $\mathrm{SU}(n)\subset U(n)$ 内, 这是实的可定向的自然的类比. 这是 Calabi-Yau 流形的第二个用度量来表示的定义.

4. 卡拉比猜想

卡拉比提出了下面的猜想: 任给一个复维数为 n 的凯勒流形, 以及任意的复定向, 必存在一个函数 u 和一个新的凯勒度量 $\tilde{g}$, 在局部坐标下表示为

$$\tilde{g}_{a\bar{b}}=g_{a\bar{b}}+\frac{\partial^2 u}{\partial z^a\partial\bar{z}^b},$$

① 注意记号 $g_{a\bar{b}}$ 的下标是 $\bar{b}$ 而不是 b, 这表明厄尔米特内积对第二个变元是共轭线性的. —— 中译本注

而且仍与原来的复定向相容. 用方程来表示相容条件就是

$$\det\left(g_{a\bar{b}}+\frac{\partial^2 u}{\partial z^a \partial \bar{z}^b}\right)=|f|^2,$$

这里 f 就是上面讨论过的全纯定向函数. 所以, 用度量来表示的 Calabi-Yau 流形的定义就是一个可怕的完全非线性偏微分方程. 卡拉比证明了它的解的唯一性, 而丘成桐证明了这个方程解的存在性. 所以, 事实上, Calabi-Yau 流形的度量定义是由它的凯勒结构及其复定向唯一决定的.

丘成桐的定理确定了在一个流形上, 具有完整群 $\mathrm{SU}(n)$ 以及复定向的度量的空间, 对应于不等价的凯勒结构的空间. 后一个空间很容易用代数几何的技巧来探讨.

5. 物理学中的 Calabi-Yau 流形

爱因斯坦的引力理论, 即广义相对论, 建立了黎曼时空流形的度量必须满足的方程 (见*广义相对论和爱因斯坦方程*[IV.13]). 这个方程中涉及了 3 个张量: 度量张量、里奇 (Ricci) 曲率张量, 以及物质的能量动量张量. 一个里奇曲率为零的流形, 当没有物质时是这个方程的一个解, 而且是一个**爱因斯坦流形**的特例. 一个具有唯一的 $\mathrm{SU}(n)$ 完整群的 Calabi-Yau 流形具有零里奇曲率, 所以在广义相对论中是有意义的.

理论物理学的一个基本问题是如何把爱因斯坦理论融入粒子的量子理论中. 这个事业称为**量子引力理论**. Calabi-Yau 流形在首选的量子引力理论即*弦论*[IV.17 §2]方面起突出的作用.

在弦论中, 基本的对象是 1 维的 "弦". 弦在时空里的运动用一个 2 维的轨迹来描述, 这个轨迹称为**世界叶** (worldsheets), 所以世界叶的每一点都用此点在时空里的位置来标记. 于是, 可以这样来构造弦论, 即把它作为从 2 维的*黎曼曲面*[III.79]到时空流形 M 的映射的量子场论. 对这个 2 维的曲面应该赋以一个黎曼度量, 而可供考虑的黎曼度量形成了一个无限维空间. 这意味着我们必须在 2 维中解决量子引力的问题 —— 这个问题和它的 4 维的同伴一样, 是太难了. 然而, 如果 2 维的世界叶理论是共形的 (即在局部的尺度变换下是不变的), 则留下的就只是一个共形不等价度量的有限维空间, 而这个理论就能适当地定义.

Calabi-Yau 条件就是从这样的考虑中产生的. 要求 2 维理论是共形的, 使得弦论有意义, 实质上就是要求时空的里奇张量为零. 这样, 2 维条件引导出一个时空方程, 而且恰好就是无物质的爱因斯坦方程. 对这个条件还要再加上一个 "唯象的" 判据, 即这个理论应该具有 "超对称", 就是要求时空流形 M 是复流形. 这两个条件合在一起意味着 M 是一个以 $\mathrm{SU}(n)$ 为完整群的复流形, 就是一个 Calabi-Yau 流形. 根据丘成桐的定理, 这种 M 的选择很容易用代数几何的方法来描述.

我们要提醒一下，弦论有一种提炼，称为"拓扑弦"，对它也可以给予一个严格的数学框架. Calabi-Yau 流形既是辛 (symplectic) 的又是复的，这就会导出拓扑弦的两个版本，分别称为 A 和 B，而都可以与 Calabi-Yau 流形连接起来. 镜面对称是一个值得注意的现象，它把 A 版本的 Calabi-Yau 流形与另一个完全不同的"镜面伙伴"的 B 版本连接起来. 这样一种等价关系的数学后果是极为丰富的 (更详细的介绍，可见镜面对称[IV.16]. 与本文的讨论相关的其他概念，可见条目辛流形[III.88]).

变　分　学
(The Calculus of Variaton)

见变分法 [III.94]

III.7 基　数
(Cardinals)

集合的基数是集合的大小的一种度量. 更准确地说，如果两个集合之间有一个双射，就说两个集合有相同的势 (cardinality)，即相同基数. 那么，有些什么样的基数呢?

首先，我们有限势，就是有限集合的势：一个集合具有"势 n"，如果它恰好有 n 个元素的话. 然后就是可数与不可数集合[III.11]，所有这种可数集合都有同样的势 (这可以从可数性的定义得出)，通常记为 $\aleph_0$. 例如自然数集合、整数集合、有理数集合都具有势 $\aleph_0$. 然而实数集合是不可数的，所以其势不是 $\aleph_0$. 事实上，它的势记为 $2^{\aleph_0}$.

可以证明，基数可以相加和相乘，甚至可以取其他基数的幂，所以 $2^{\aleph_0}$ 不是一个单独的记号 [而是对一个势为 $\aleph_0$ 的集合进行某种运算的结果]. 更多的细节和解释可见条目集合理论[IV.22 §2].

III.8 范　畴
(Categories)

Eugenia Cheng

研究群[I.3 §2.1] 和向量空间[I.3 §2.3] 的时候，我们特别注意两个群或两个向量空间之间的某种映射，群之间重要的映射是同态[I.3 §4.1]，而向量空间之间重要的映射是线性映射[I.3 §4.2]. 这些映射之所以重要，在于它们是"保持结构"的函数，

例如, 若 ϕ 是由群 G 到群 H 的一个同态, 则对于 G 的任一对元素 g_1, g_2, ϕ 将会“保持乘法”, 就是 $\phi(g_1g_2)=\phi(g_1)\phi(g_2)$. 类似地, 线性映射将会保持加法与乘以标量.

保持结构的映射这个概念的应用领域比这两个例子广得多, 而范畴理论的目的之一就是要弄明白这种映射的一般性质. 例如, 若 A, B 和 C 是某个给定类型的数学结构, 而 f 和 g 分别是由 A 到 B 和由 B 到 C 的保持这种结构的映射, 则它们的复合 $g\circ f$ 就是由 A 到 C 的保持结构的映射. 就是说, 保持结构的映射可以**复合**(至少是当一个映射的值域等于另一个映射的定义域时可以复合). 我们也时常用保持结构的映射来决定何时可以把两个同一类型的结构视为“本质上相同”, 如果有一个由 A 到 B 的保持结构的映射, 而且其逆也是保持结构的映射, 就说 A 和 B 是**同构的**[也就是“本质上相同”的].

范畴就是允许我们抽象地来讨论这样一些性质的数学结构. 它包含了一组**对象**, 还有这些对象之间的**态射**(morphism). 就是说, 如果 a 和 b 是此范畴的两个对象, 范畴中还包括了这两个对象之间的一组态射, 也有态射的复合这个概念, 若 f 是由 a 到 b 的态射, g 是由 b 到 c 的态射, 则存在 f 和 g 的一个复合为由 a 到 c 的态射. 这个复合必须是结合的. 此外, 对每一个对象 a 都存在一个“恒等态射”, 它的性质是: 如果把它与任意态射 f 复合起来, 则仍会得到 f.

正如前面的讨论暗示的那样, 范畴的一个例子是群的范畴. 这个范畴的对象就是群, 而态射就是群同态, 复合和恒等态射都如我们习惯的那样定义. 然而, 下面的例子表明, 绝非所有的范畴都是这样的:

(i) 可以这样来构造一个范畴, 其对象为自然数, 而由 n 到 m 的态射是所有具有实数元的 $n\times m$ 矩阵, 态射的复合和恒等态射就定义为矩阵的乘法和恒等矩阵. 正常情况下, 不会把 $n\times m$ 矩阵想成一个由数 n 到数 m 的映射, 然而范畴的公理是得到了满足的.

(ii) 任何集合都可以变成一个范畴, 对象就是此集合的元素, 而由 x 到 y 的态射就是断言“$x=y$”. 也可以把一个有序集合变成一个范畴, 而令由 x 到 y 的态射为断言“$x\leqslant y$”(“$x\leqslant y$”和“$y\leqslant z$”的“复合”则是“$x\leqslant z$”).

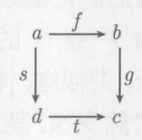
(iii) 任意的群也可以像下面那样变成一个范畴, 它仅有一个对象, 而由此对象到其自身的态射就是群中的元素, 态射的复合则定义为群中的乘法.

(iv) 还有一个明显的范畴, 其对象为拓扑空间[III.90], 态射则为连续函数. 还有一个不那么明显的范畴, 其对象和上面说的一样, 但是不以连续函数而以连续函数的同伦类[IV.6 §2] 为态射.

态射也叫**映射**. 然而正如上面的例子表明的那样, 范畴中的映射与我们熟悉的映射的样子可以很不相像. 这些映射也称为**箭头**, 这样的称呼部分地是为了强调一般的范畴具有比较抽象的特性, 部分地则是因为将用箭头来“画”出态射.

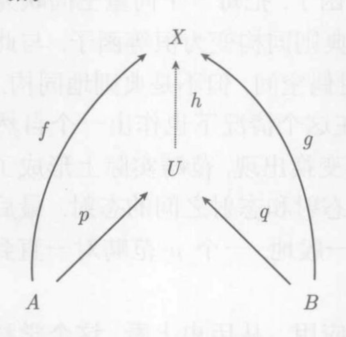
"对象和态射" 这种一般框架和语言使我们能够找出和研究那些仅仅依赖于范畴的 "形状" 的特性, 就是仅依赖于态射和它们所满足的方程的那些特性. 这里的思想就是: 既作出一般的论据, 然后可以用于所有的具有这个特定的结构特性范畴, 同时, 在特定的环境下, 又可以不必进入所讨论的结构的细节. 使用前者, 达到后者, 有时被说成是 "抽象的胡说八道", 认为这种说法是亲切也好, 认为它是开玩笑也好.

正如上面说的, 范畴中的态射时常用箭头画出来, 所以, 由 a 到 b 的态射 f 就画成 $a \xrightarrow{f} b$, 而复合则用箭头画成 $a \xrightarrow{f} b \xrightarrow{g} c$. 这个记号大大地简化了复杂的计算, 而产生出所谓可换图式, 而这种图书式又时常是与范畴相联系的, 两个复合的等式如 $g \circ f = t \circ s$ 就被说成是下面的图式是可换的, 就是说下图中由 a 到 c 的两条路径会给出同样的复合.



想要证明一长串的复合等于另一长串, 时常就变成在空白处 "填上" 已知是可换的小图式. 此外, 许多重要的数学概念都可以用可换图式来表示, 下面是一些例子: 自由群、自由环、自由代数、商、乘积、不相交并、函数空间、定向极限和逆极限、完备化、紧化和几何实现.

现在我们来看一下不相交并是怎样用可换图式来表示的. 说集合 A 和 B 的不相交并就是一个集合 U 再带上两个态射 $A \xrightarrow{p} U$, $B \xrightarrow{q} U$, 使得对于任意一个集合 X 和两个态射 $A \xrightarrow{f} X$, $B \xrightarrow{g} X$, 必有唯一的态射 $U \xrightarrow{h} X$, 使下面的图式是可换的:



这里的 p 和 q 告诉我们 A 和 B 是怎样插到不相交并里面去的, 而定义中 "使得对于" 以下的那一段话是一个**泛性质**(universal property), 它表示了一个事实: 给定一个由不相交并到另一个集合的函数, 恰好就是在每一个个别的集合上给定一个函数, 这就完全地刻画了不相交并 (而这个不相交并确定到只相差一个同构). 另一种观点是, 泛性质表示了一个事实, 不相交并是把两个集合映射到另一个集合的 "最自由" 的方式, 既不增加任何信息, 也不使任何信息崩溃. 泛性质对于范畴理论中描述结构的方式多少有点 "典则的" 的味道, 而且是其核心 (参看条目*几何和组合群论*[IV.10] 中关于自由群的讨论).

范畴中另一个关键的概念是**同构概念**. 可以期望, 同构应该定义为一个具有双侧逆的态射. 在一个给定的范畴中, 同构的对象应该看成是 "关于这个范畴是相同

的对象”. 这样, 范畴提供了一个框架, 其中对象的最自然的分类的方法是容许 “相差一个同构”.

范畴也是某一类数学结构, 所以范畴本身也构成一个范畴 (但是对于范畴的大小要有限制, 以避免罗素类型的悖论). 保持范畴结构的态射, 称为**函子**. 换句话说, 由范畴 X 到范畴 Y 的函子 F 把 X 的对象变为 Y 的对象, 把 X 的态射变为 Y 的态射, 而且把 X 的恒等态射 a 变成 Y 的恒等态射 Fa, X 的态射 f 和 g 的复合变成 Y 的态射 Ff 和 Fg 的复合. 函子的一个重要的例子是把指定了标记点 s 的拓扑空间 S 映到其基本群 $\pi_1(S\,,\,s)$ 的函子. 代数拓扑学的基本定理之一是两个拓扑空间之间的连续映射 (并规定映标记点为标记点) 生成基本群的一个同态.

进一步还有函子之间的态射, 即称为**自然变换**的概念, 它类似于拓扑空间之间的映射的同伦的概念: [在拓扑空间的情况下], 给定两个连续映射 $F\,,\,G:X\to Y$, 一个由 F 到 G 的同伦对于 X 的每一点 x 都给了我们一个 Y 中的由 Fx 到 Gx 的路径; 类似地, [在范畴的情况下], 给定了两个函子 $F\,,\,G:X\to Y$, 一个由 F 到 G 的自然变换, 就对 X 的每一个对象 x 给出 Y 中的一个把 Fx 变为 Gx 的**态射**. [同伦情况的以下事实, 即可换条件]也有一个类比: 在同伦的情况, X 中的路径在 F 下的像必定会连续地变为这个路径在 G 下的像, 而不会穿过 Y 中的 “洞”, 避免落入洞中, 这个事实在范畴的情况下可以用目标范畴 Y 中的一个正方形的可换性来表示, 这个可换性称为 “自然性条件”.

自然变换有一个例子, 说明了以下事实: 每一个向量空间必**典则地**同构于其双重对偶; 有一个由向量空间的范畴到其自身的一个函子, 把每一个向量空间映为其双重对偶, 而且有一个自然变换, 把这个函子通过典则同构变为恒等函子. 与此形成对比的是: 每一个有限维向量空间都同构于其对偶空间, 但不是典则地同构, 因为这个同构用到了基底的任意选取; 如果我们想在这个情况下也作出一个自然变换, 就会发现自然性条件不再成立了. 由于有自然变换出现, 范畴实际上形成了一个 2 **范畴**, 它是范畴的 2 维的推广, 其中有对象、态射和态射之间的态射. 最后这个态射之间的态射可以看成是 2 维的态射. 更加一般地, 一个 n 范畴对一直到 n 的每一个维数都有态射.

范畴及其语言在许多其他的数学分支中都有应用. 从历史上看, 这个学科与代数拓扑学紧密相关, 这些概念是艾伦伯格 (Eilenberg) 和麦克莱恩 (MacLane) 在 1945 年提出的. 后来跟着就在代数几何、理论计算机科学、理论物理和逻辑学中都有了应用. 由于范畴理论的抽象本性以及不依赖于其他数学分支, 可以看成是 “基础性的”. 事实上, 也有人建议, 以范畴理论来作为数学基础的另一个候补对象, 把态射作为最基本的概念, 而所有其他概念都要由它派生出来, 而不像在集合论基础[IV.22 §4] 里面使用集合的属于关系作为最基本的概念.

类域理论
(Class Field Theory)

见从二次互反性到类域理论 [V. 28]

上 同 调
(Cohomology)

见同调与上同调 [III. 38]

III.9 紧性与紧化
(Compactness and Compactification)

陶哲轩 (Terence Tao)

大家都知道在数学中, 有限集合和无限集合的性态可以很不相同. 例如下面三个命题, 容易看到, 当 X 为有限集合时都为真, 但当 X 为无限集合时都不真.

所有函数都是有界的. 若 $f: X \to \mathbf{R}$ 是 X 上的实值函数, 则 f 必定是有界的 (即存在一个有限数 M 使得对于所有的 $x \in X$, 均有 $|f(x)| \leqslant M$).

所有的函数都能达到最大值. 若 $f: X \to \mathbf{R}$ 是 X 上的实值函数, 则必存在至少一个点 $x_0 \in X$, 使得对于所有的 $x \in X$, 均有 $f(x_0) \geqslant f(x)$.

所有序列都有常值子序列. 若 $x_1, x_2, x_3, \cdots$ 是 X 中的一个点序列, 则必存在它的一个子序列 $x_{n_1}, x_{n_2}, x_{n_3}, \cdots$ 取常值. 换言之, 必有某个 $c \in X$ 使得 $x_{n_1} = x_{n_2} = \cdots = c$ (这个事实有时称为**无限抽屉原则**①).

第一个命题 —— 有限集合上的所有函数都有界 —— 可以看成是**局部到整体原理**的一个非常简单的例子. 它的假设是一个 "局部" 的有界性的论断, [由此假设可得] $|f(x)|$ 对于每一个点 $x \in X$ 分别都有界, 但是这个界一般地是依赖于 x 的. 现在结论是 "整体" 的有界性: $|f(x)|$ 对于所有的 $x \in X$, 界于**单独一个** M .

迄今, 我们仅限于对象 X 是一个集合的情况. 但是在许多数学领域里, 我们愿意对于对象集合再赋以附加的结构, 例如赋以一个*拓扑*[III.90]、一个*度量*[III.56] 或者一个*群结构*[I.3 §2.1]. 当这样做了以后, 我们的对象会展现出某些类似于有限集合的性质 (特别是, 也会有局部到整体原理), 虽然这些集合现在是无限集合. 在拓扑空间和度量空间的范畴中, 这种 "几乎有限" 对象就是**紧空间**(在其他范畴里, 也

① 我国文献习惯上所说的抽屉原则, 在许多英文文献中称为 "鸽笼原则"(pigeonhole principle). —— 中译本注

有 “几乎有限” 的对象, 例如在群的范畴里就有**投射有限群**(profinite groups)[1]的概念, 对于赋范空间[III.62] 之间的线性算子[III.50], 则有紧算子的概念, 就是 “几乎有限秩” 的算子, 等等).

闭单位区间 $X = [0\ ,\ 1]$ 是紧集合的一个好例子. 它是一个无限集合, 所以前面的三个命题对于这个 X 都不真. 但是如果引入一些拓扑概念, 如连续性和收敛性, 就可以把这些命题恢复成以下的形式:

所有的连续函数都是有界的. 如果 $f: X \to \mathbf{R}$ 是 X 上的实值连续函数, 则 f 必定是有界的 (这又是一种类型的局部到整体原理: 如果一个函数局部地变化不太大, 则它在整体上变化也不太大).

所有的连续函数必达到最大值. 如果 $f: X \to \mathbf{R}$ 是 X 上的实值连续函数, 则必定存在至少一点 $x_0 \in X$, 使得对于所有的 $x \in X$, 均有 $f(x_0) \geqslant f(x)$.

所有的点序列都有收敛的子序列. 若 $x_1, x_2, x_3, \cdots$ 是 X 中的一个点序列, 则必存在它的一个子序列 $x_{n_1}, x_{n_2}, x_{n_3}, \cdots$ 收敛于某点 $c \in X$(这个命题称为**波尔扎诺–魏尔斯特拉斯定理**).

对于这些命题, 我们还可以加上第四个 (但是和前三个不同, 第四个在有限集合情况下的类比是颇为平凡不足道的).

所有开覆盖都有有限子覆盖. 若 Υ 是一族开集合, 其并包含了整个 X(这时 Υ 称为 X 的一个开覆盖), 则必存在 Υ 的一个有限子集合 $V_{n_1}, V_{n_2}, \cdots, V_{n_k}$ 仍然覆盖 X.

这四个拓扑命题对于如像开的单位区间 $(0\ ,\ 1)$ 和实轴 $\mathbf{R}$ 这样的集合都不真, 这一点可以用简单的反例来证明. **海涅–波莱尔**定理指出, 当 X 是欧几里得空间 $\mathbf{R}^n$ 的子集合时, 上面这四个命题, 当 X 在拓扑上是闭的有界集合时, 都是真的, 否则都不真.

这四个命题互相有密切的关系. 例如, 如果知道了 X 的所有序列都包含有收敛的子序列, 就可以很快导出其上所有连续函数都有最大值. 这一点可以这样来证明: 先作一个最大化序列 —— 就是 X 中的点 x_n 的序列, 使得 $f(x_n)$ 趋向于其最大值 (准确一点应该说是趋向于其上确界)—— 然后再去研究其收敛的子序列, [就可以完成证明]. 事实上, 对 X 给以比较温和的假设 (例如设它是一个度量空间), 就可以从这四个命题的任意一个导出其余三个.

如果允许说一点稍嫌过分简单的话, 我们说如果对于拓扑空间 X, 只要以上四个命题有一个成立 (从而所有的都成立), 就说 X 是一个**紧空间**. 因为这四个命题一般地并不完全等价, 所以紧性的形式定义只采用第四个命题: 若每一个开覆盖都有有限的子覆盖, [就说 X 为紧空间]. 还有紧性的其他概念, 例如以第三个命题为

[1]有人译为投射有限群. 这是一类在某种意义下由有限群合并而成的拓扑群, 因为我们可以定义它为离散的有限群的**反向系**(inverse system) 的**投射极限**(projective limit). —— 中译本注

基础, 就得到列紧性, 但是这里的区别有点技术化, 所以我们略过这些区别不谈了. 紧性是空间的一个强有力的性质, 它以多种方式用于数学的许多不同领域. 其中它有一个用处就是用它来建立局部到整体原理: 先对一个函数或其他的什么量建立起局部的控制, 再用紧性把它推向整体的控制. 另一个用处是用它来找出一个函数的最大值和最小值. 这在**变分法**[III.94] 中特别有用. 第三个用法是在处理发散序列时用它来部分地恢复极限的概念, 这时需要接受过渡到子序列的必要性 (然而, 不同的子序列可能收敛到不同的极限; 紧性只能保证极限点的存在, 而不能保证其唯一性). 一个对象的紧性常会带来其他对象的紧性, 例如紧集合在连续映射下的像仍然是紧的; 有限多个甚至无限多个紧集合的乘积仍然是紧的. 最后这个结果称为**吉洪诺夫**(Andrei Nikolaevich Tikhonov, 1906–1993, 前苏联数学家)**定理**.

当然, 许多有趣的空间并不是紧的. 一个明显的例子就是实数轴 $\mathbf{R}$, 因为其中有一个序列 $1, 2, 3, \cdots$, 它"总想跑出直线", 而一个收敛子序列也没有留下来. 然而我们可以多加几个点到这个空间上去, 由此来恢复紧性, 这个过程称为**紧化**. 例如我们可以在实数轴的每一端各加上一个点使它紧化, 这两个点叫做 $+\infty$ 和 $-\infty$. 这样得到的对象称为**扩张的实数直线**$[-\infty, +\infty]$, 可以很自然地给以一种拓扑, 它基本上定义了什么叫收敛于 $+\infty$ 或 $-\infty$. 扩张的实数直线是紧的. 每一个扩张的实数的序列 x_n 都有一个收敛的子序列, 或者收敛于 $+\infty$, 或者收敛于 $-\infty$, 或者收敛于某一个有限的数. 这样, 应用扩张的实数把实数直线紧化, 就可以把极限推广, 使得不是实数的东西也可以作为极限. 这样来处理扩张的实数, 比较通常的实数当然有小缺点 (例如两个 [扩张后的] 实数不一定可以相加, $+\infty$ 和 $-\infty$ 的和就无定义). 能够对原来是发散的序列取极限可能是很有用的, 特别是在无穷级数理论和反常积分理论中有用.

结果是同一个非紧的空间可以有不同的紧化. 例如, 应用球极射影可以把实数直线和除去了一个点的圆周在拓扑上等同起来 (例如, 利用下面的映射把实数 x 映为一点 $\left(x/\left(1+x^2\right), x^2/(1+x)^2\right)$, 则 $\mathbf{R}$ 被映为以 $(0, 1/2)$ 为圆心、$1/2$ 为半径的圆周, 但是除去了北极 $(0, 1)$). 如果再把这个缺的点补上, 就得到实数直线的**一点紧化** $\mathbf{R}\cup\{\infty\}$. 更一般地说, 任何一个合理的拓扑空间 (例如一个局部紧的豪斯道夫空间[①]) 都有好几个紧化, 从"最小的"紧化, 即只补一点的紧化, 即一点紧化 $X\cup\{\infty\}$, 到"最大的"紧化: Stone- Čech 紧化[②]βX, 要添加大量的点. 自然数集合 $\mathbf{N}$ 的 Stone-Čech 紧化 $\beta\mathbf{N}$ 就是超滤子 (ultrafilters) 空间, 在数学的更依赖于无穷的部分里很有用.

可以利用紧化来区别一个空间里不同类型的发散性. 例如, 扩张的实数直线里

① 豪斯道夫空间就是不同点必有不相交的邻域的拓扑空间. —— 中译本注

② Stone, 就是 Marshall Harvey Stone , 1903–1989, 美国数学家; Čech, 就是 Eduard Čech, 1893–1960, 捷克数学家. —— 中译本注

发散于 $+\infty$ 和发散于 $-\infty$ 是不一样的. 按照同样的精神, 把 $\mathbf{R}^2$ 紧化为*射影平面*[I.3 §6.7]以后, 就可以区别一个序列沿着 (或近于)x 轴的发散与沿着 (或近于)y 轴的发散. 当序列以不同方式发散会展现不同的性态时, 这种紧化就会自然地出现.

紧化的另一个用途是, 它时常能够严格地把一种类型的数学对象看成其他对象的极限. 例如, 只要把圆周的空间适当紧化, 使之包括直线, 就可以把直线看成越来越大的圆周的极限. 这种前景使我们能够从关于圆周的定理导出关于直线的定理, 或者反过来从关于直线的定理导出关于很大的圆周的定理. 再举在一个很不相同的数学领域里的例子, 狄拉克的 delta 函数本来不是严格意义下的函数, 但是在某些函数空间里, 例如在某种*测度*[III.55] 空间或者*广义函数*[III.18] 空间里, 存在某种 (局部的) 紧化, 使我们可以把 delta 函数看成经典的函数的极限. 我们还可以利用紧化把连续的东西看成离散的东西的极限, 例如循环群序列 $\mathbf{Z}/2\mathbf{Z}$, $\mathbf{Z}/3\mathbf{Z}$, $\mathbf{Z}/4\mathbf{Z}$, $\cdots$ 就可以紧化为圆群 (circle group)$\mathbf{T}=\mathbf{R}/\mathbf{Z}$. 这些简单的例子可以推广为紧化的很精巧的例子, 而在几何、分析与代数中有很多应用.

III.10 计算复杂性类
(Computational Complexity Classes)

理论计算机科学的最基本的挑战之一就是要决定为了完成一项给定的计算任务, 需要多少计算资源. 最基本的资源是**时间**, 或者与此等价, 就是 (在给定的硬件条件下) 执行完成这个任务的最有效的算法需要多少步. 特别重要的是随着这项任务的输入的大小, 这种时间将按怎样的尺度增加, 例如要把一个 $2n$ 位的整数作因数分解, 比把一个 n 位数作因数分解所需时间要长多少? 与计算的可行性相关的另一个资源是**存储**. 我们要问: 一个计算机执行一个算法需要多大的存储空间, 又怎样使它最小. 一个**复杂性类**就是能够在一定限制的资源下完成的计算问题的集合. 例如复杂性类 $\mathcal{P}$ 就包括了所有能够在 "多项式时间" 内完成的问题, 这就是说, 存在一个正整数 k, 使得如果问题的大小是 n(在上面的例子中, 大小就是要分解的整数的位数), 则计算可以在最多 n^k 步之内完成. 一个问题属于复杂性类 $\mathcal{P}$ 当且仅当输入的大小按尺度增加一个常数因子时, 解决这个问题的时间也按尺度增加一个常数因子. 这类问题的一个好例子是两个 n 位数的乘法, 如果使用通常的长乘法, 则在把 n 换成 $2n$ 时, 所需的时间要增加因数 4.

设给了一个正整数, 并且是两个素数 p, q 的积. 要决定 p 和 q 有多难? 谁也不知道, 但是有一点容易看到, 如果已知两个数 p 和 q, 则容易验证 (至少是对计算机而言)pq 确实等于 x. 事实上, 我们已经看到, 长乘法需要多项式时间, 而把相乘的

答案与 x 比较甚至更容易一点. 复杂性类 $\mathcal{NP}$ 是由这样一些计算任务构成的: **验证**其结果的正确性只需要多项式时间, 虽然在多项式时间内, 不一定就能**找出**这个结果. 值得注意的是, 虽然有这个基本的区别, 谁也不知道如何证明 $\mathcal{P} \neq \mathcal{NP}$, 这个问题普遍认为是理论计算机科学的最重要的问题.

我们再简单地提一下另外两个重要的复杂性类. 第一个类记为 $\mathcal{PSPACE}$. 它包含了这样一些问题, 解决它们所需的存储最多按问题的大小呈多项式增长. 结果, 这是与一类博弈 (如下棋) 的计算机策略相关的自然的复杂性类. 第二个复杂性类记为 $\mathcal{NC}$, 则是所有这样的布尔函数的集合, 这种布尔函数可以用 "具有多项式大小与深度为 $\log n$ 的多项式的回路"①来计算. 这个类是一类问题的模型, 这类问题可以用并行处理很快解决. 一般说来, 复杂性类这个概念, 在刻画具有共同的有趣的特性的一大类问题时常有非常好的作用. 另一个值得注意的事情是每一个复杂性类中, 常有 "最难的" 问题, 其解答常可转化为类中所有其他问题的解答. 这种问题被说成是对于这个类为**完备的**.

这些问题, 还有其他的复杂性类, 将在条目计算复杂性[IV.20] 中讨论. 在网站

http://qwiki. stanford. edu/wiki/Complexity_Zoo

中可以找到许多进一步的复杂性类以及它们的简单定义.

连 分 数

(Contined Fractions)

见欧几里得算法和连分数 [Ⅲ.22]

III.11 可数与不可数集合

(Countable and Uncountable Sets)

无限集合在数学中时时出现, 自然数、完全平方数、素数、整数、有理数、实数等等都构成无限集合. 人们时常自然地想要比较这些集合的大小, 人们直觉地感觉自然数的集合 "小于" 整数的集合 (因为后者还包含了负数), 但是比完全平方数的集合就大得多 (因为一个典型的大数不大可能是完全平方数). 但是我们能在精确的意义下比较它们的大小吗?

① 按照维基百科的说法, 回路有两个量度其复杂性的指标: 大小, 就是其中所包含的 "门" 的多少; 深度, 则是其中最长的有向路径的长度. 详见 http://en. wikipedia. org/wiki/Arithmetic_circuit#Definitions. —— 中译本注

一个明显的解决这个问题的方法建立在我们关于有限集合的直觉上. 若 A 和 B 是两个有限集合, 有两个方法来比较它们的大小. 一是去数它们的元素的个数, 于是会得到两个非负的整数 m 和 n, 然后看一看, 是 $m < n$, 还是 $m = n$, 还是 $m > n$. 但是还有另一个重要的方法, 不需要确知 A 或 B 的大小, 这就是把 A 的元素和 B 的元素配对, 直到有一个集合的元素被取尽为止, 元素先被取尽的集合就是较小的集合, 如果总是打成平手, 这两个集合就是一样大小.

第二个方法稍作修改以后, 也可以用于无限集合. 如果两个集合之间有一个一一对应, 就说它们的大小相同. 我们将会看到, 这是一个重要而又有用的定义, 虽然它有一些推论会让我们一开始感到有点怪. 例如, 在自然数集合和完全平方数集合之间有一个显然的一一对应: 对每一个 n, 让 n^2 与之相应. 这样, 按照定义, 平方数和自然数应该是 "一样多". 类似于此, 素数和自然数也是一样多, 对于 n, 有第 n 个素数与它对应[①].

关于 $\mathbf{Z}$ 又如何? 似乎它应该是 $\mathbf{N}$ 的两倍大, 但是我们又能找到二者之间的一一对应. 只需把整数列表如下: $0, 1, -1, 2, -2, 3, -3, \cdots$, 然后把它们与自然数配对, 方法是明显的, 1 配 0, 2 配 1, 3 配 -1. 4 配 2, 5 配 -2, 等等.

如果一个无限集合与自然数集合有相同的大小, 就称为**可数集合**. 正如上面的例子所说明的, 这和说这个集合的元素可以**列表**是完全一样的. 实际上, 如果把一个集合的元素列表为 $a_1, a_2, a_3, \cdots$, 则我们的一一对应就是 n 与 a_n 对应. 值得注意的是, 当然有一些我们想用的列表是不行的, 例如, 可以试着把 $\mathbf{Z}$ 列表为 $-3, -2, -1, 0, 1, 2, 3, 4, \cdots$ [想一想为什么不行]. 所以重要的是要认识到, 当我们说一个集合是可数集合时, 并不是我们想用的**哪一个**列表方法都能行, 甚至也不是说, 那些明显的列表方法是行的, 我们只是说, 集合的元素有**某种**列表的方法. 这与有限集合完全不同, 对于有限集合, 如果应用某一种配对的方法有一个集合留下了一些元素, 我们就知道, 这两个集合之间不会有一一对应. 上面出现的那些 "奇怪的" 推论主要是来自于此.

现在我们已经确定了某些看来比 $\mathbf{N}$ 小, 或者比 $\mathbf{N}$ 大的集合, 实际上是可数集合, 那么我们再转到一个看起来 "大得多" 的集合, 即有理数集合 $\mathbf{Q}$. 我们怎么能够希望把所有的有理数列成一个表呢? 归根结底, 在任意两个有理数之间可以找到无穷多个其他有理数, 所以当想去把它们列成一个表的时候, 很难不漏掉哪一个. 然而, 尽管看起来很值得注意, **确实可以**把有理数列成一个表. 关键的思想是在列表的时候, 要使这个有理数的分数表示的分子和分母二者 (按绝对值) 都小于某个定数 k. 这样列表就容易了, 因为符合这个条件的有理数只有有限多个. 所以, 我们就按下面次序进行: 首先排列分子分母都最多为 1 的有理数, 再排分子分母最多为 2

①对于很好的自然数集合, 有一个 "密度" 的定义可能有用. 按照这个定义, 偶数的密度是 1/2, 而平方数和素数的密度都是 0. 然而密度概念并不是我们这里讨论的大小的概念.

的, 仿此以往 (注意不要重复任意的数, 例如排列了 1/2 以后, 就不要再排 2/4 , 3/6 了). 这就会给出例如下面的列表:

$$0\,,\,1\,,\,-1\,,\,2\,,\,-2\,,\,\frac{1}{2}\,,\,-\frac{1}{2}\,,\,3\,,-3\,,\,\frac{1}{3}\,,\,-\frac{1}{3}\,,\,4\,,$$

$$-4\,,\,\frac{1}{4},\,-\frac{1}{4},\,\frac{3}{4},\,-\frac{3}{4},\,\frac{4}{3},\,-\frac{4}{3},\,5\,,\,-5\,,\cdots.$$

我们可以用同样的思想来排列看起来甚至更大的集合, 例如代数数集合 (即所有满足整数系数的多项式方程的实数, 如满足 $x^2-2=0$ 的 $\sqrt{2}$). 实际上, 注意到每一个多项式方程只有有限多个根 (这些根可以列成表) 所以需要我们去做的就只是把多项式列成表 (然后在每一个多项式里面依次列出所有的根就行了). 在把多项式列表的时候, 又可以用上面的办法: 对于每个定数 d, 排列那些次数不超过 d, 系数之模最多也为 d 而且还没有排列过的多项式.

基于以上的例子, 可能会猜想, 每一个无限集合都是可数的. 但是康托[VI.54]的一个漂亮的论据, 称为 "对角线" 方法的论证方法, 说明实数集合是不可数的. 设想实数集合有一个列表的方法: $r_1\,,\,r_2\,,\,r_3\,,\cdots$. 我们的目的是要证明这个列表不可能包含所有的实数, 所以要造出一个不在这个表上的实数. 怎样做这件事呢? 把每一个 r_i 都写成例如一个无穷十进小数, 现在来造出一个实数 s, 它的小数点后的第一位数码要选得和 r_1 的第一位数码不同. 这就已经保证了 s 不可能等于 r_1(为了避免递推地出现 9 等等, 最好 s 的第一位数码连 9 和 0 也不要取). 然后, s 的第二位要取一个与 r_2 的第二位不同的数码, 这就保证了 s 也不可能等于 r_2. 像这样做下去, 最后就得出一个不在所说的列表中的实数 s, 不论 n 是多少, s 都不可能等于 r_n, 因为它们在小数点后的第 n 位不同!

当这样来确定一个对象时 (如要选择 s 的各位数码那样), 都可以采用上面的论证方法而有 "无穷多个独立的选择要作". 例如, 让我们用同样的思想来证明自然数集合 $\mathbf{N}$ 的子集合的个数是不可数的. 假设我们能够把 $\mathbf{N}$ 的所有子集合列成一个表 $A_1,\,A_2,\,A_3,\cdots$. 要定义 $\mathbf{N}$ 的一个新的子集合 B, 使它不等于任何一个 A_n. 把 1 放进 B 中, 当且仅当 1 不在 A_1 中 (这就保证了 B 不等于 A_1), 把 2 放进 B 中, 当且仅当 2 不在 A_2 中, 如此等等. 有趣的是, 我们可以把这个集合 B 写下来: $B=\{n\in\mathbf{N}:n\notin A_n\}$, 这表明 B 很像罗素悖论里的集合.

可数集合是 "最小的" 无限集合. 然而实数集合绝非 "最大的" 无限集合. 事实上, 上面的论证说明任意一个集合 X 都不能与它自己的所有子集合的集合一一对应. 所以, 实数集合的所有子集合的集合 "严格地大于" 实数集合, 等等.

可数性的概念是非常富有成果的, 值得记在心上. 例如, 设我们想知道是否所有实数都是代数数. 要想证明一个特定的实数真正是超越数[III.41] 而不是代数数, 这是一个很难的练习 (见刘维尔定理和罗特定理[V.22] 就可以知道这是怎样做的),

但是上面的论证使得证明超越数的存在变成极为不足道的事情. 事实上, 实数集合是不可数的, 而代数数的集合则是可数的. 此外, 这个论证还说明 "绝大多数" 实数都是超越数, 代数数只占了实数的极小一部分.

III.12　C^*-代数
(C^*-Algebras)

一个巴拿赫空间[III.62] 既是一个向量空间[I.3 §2.3], 又是一个度量空间[III.56], 所以巴拿赫空间的研究就是线性代数和分析的混合物. 但是, 如果我们注意具有更多代数结构的巴拿赫空间, 就会得到代数和分析的更复杂的混合物. 特别是, 虽然巴拿赫空间的任意两个元素都可以相加, 而一般地不能相乘, 但是有时候是可以的. 一个同时具有乘法结构的向量空间称为一个代数, 而如果这个向量空间还是巴拿赫空间, 且它的乘法还有下面的性质, 就称它为一个**巴拿赫代数**: 对任意两个元素 x 和 y, $\|xy\| \leqslant \|x\|\,\|y\|$(这个名称并不反映历史的真实, 因为巴拿赫代数的理论并不是巴拿赫搞出来的, 称它为盖尔范德 (Israel Moiseevich Gelfand, 1913–2009, 前苏联数学家) 代数更适当.

C^*-代数就是一个带有对合 (involution) 的巴拿赫代数. 对合就是这样一个函数, 它让每一个元素 x 都对应于另一个元素 x^*, 并使对于任意两个元素 x 和 y 都有以下的性质成立: $x^{**} = x$, $\|x^*\| = \|x\|$, $(x+y)^* = x^* + y^*$, $(xy)^* = y^*x^*$. C^*-代数的基本的例子是定义在希尔伯特空间[III.37]H 上的所有连续线性映射 T 所成的代数 $B(H)$. T 的范数 $\|T\|$ 定义为使得所有 $x \in H$ 均有 $\|Tx\| \leqslant M\,\|x\|$ 的最小常数 M. 而所说的对合把 T 变为其伴算子 T^*. 伴算子 T^* 就是这样一个线性算子: 对于 H 中任意两个元素 x 和 y 均有 $(x\,,\,Ty) = (T^*x\,,\,y)$(可以证明, 恰有一个算子具有这样的性质). 如果 H 是有限维空间, 则 T 可以想作一个 $n \times n$ 矩阵, n 是一个整数, 这时, T^* 是 T 的转置矩阵的复共轭.

盖尔范德和奈马克 (Mark Aronovich Naimark, 1909–1978, 前苏联数学家) 的基本定理指出, 每一个 C^*-代数都可以表示为某个希尔伯特空间的 $B(H)$ 的一个子代数. 更多的信息可参看条目算子代数[IV.15 §3].

III.13　曲　　率
(Curvature)

把一个桔子切成两半, 挖掉桔肉, 再试着把剩下的半球形桔皮展平, 那就会撕破桔皮. 如果想把一个马鞍或者一片泡软的薯片展平, 这一次就会遇到相反的问题,

曲面的一部分“多出来”了, 展平的时候就会折叠起来了. 然而, 如果有一卷墙纸, 而想把它也展平, 这一次就没有困难了 (只需要把纸卷散开就行了). 球面这样的曲面, 我们说是**正向弯曲的**, 马鞍形的曲面是**负向弯曲的**, 而一片墙纸则说是**平坦的**.

注意, 在这个意义下, 一个平坦的曲面并不一定是放在平面上的. 这是因为曲率是依照曲面的内蕴几何来定义的, 在这种几何里面, 距离是依照完全位于曲面上的路径来量度的.

有许多方法把上面所说的曲率的概念弄精确, 而且使之量化, 这样, 曲面的每一点都有一个数来表示曲面在此点是“如何地弯曲”. 为了做这件事情, 曲面需要有一个*黎曼度量*[I.3 §6.10] 来定义路径的长度. 曲率这个概念也可以推广到高维情况, 这样, 我们就可以谈论一个 d 维黎曼流形的某一点处的曲率. 然而, 当维数高于 2 时, 流形在一点处弯曲的方式比较复杂, 它不是用一个数来表示, 而是用**里奇张量**来表示的. 详见条目*里奇流*[III.78].

曲率是现代几何学的基本概念之一, 不仅有上面所说的概念, 还有不同的其他定义用其他方式来说明一个几何对象如何偏离于平坦, 它也是广义相对论的不可分离的部分 (这一点将在条目*广义相对论和爱因斯坦方程*[IV.13] 中讨论).

III.14 设 计

(Designs)

Peter J. Cameron

区组设计最早是用于统计学中的试验设计, 作为一种处理试验资料的系统差异的方法. 举例来说, 设我们想要在一项农业试验中试验 7 种种子品种, 而可供使用的地块共有 21 块. 如果这些地块都被认为是完全相同的, 则最佳策略显然是每个品种种 3 块地块. 然而, 假设这 21 个地块分布在 7 个农庄里, 每个农庄有 3 个地块, 这些农庄又在不同的地方. 如果简单地在每个农庄的 3 个地块都种同样的品种, 就会丧失信息, 因为我们无法把这些区域的系统差异与每个品种的系统差异区分开来. 这时, 最好是按照以下的格式来种这些品种: 第一个农庄种 1, 2, 3[这 3 个品种]; 第二个农庄种 1, 4, 5; 然后就是 1, 6, 7; 2, 4, 6; 2, 5, 7; 3, 4, 6; 最后还有 3, 5, 6. 这种试验方案画在图 1 上面. [图中有 7 条线 (3 条是三角形的边, 3 条是中线, 第 7 条是内切圆). 每一条代表一个农庄, 我们说它们是在同一个区组内; 每条线上各取了 3 个点, 代表 3 个地块 (但是同一点可以是 3 条线的公共点); 每个点上有一个数目, 代表所种的品种, 一个点可以在 3 条线上, 表示这 3 个农庄都有一个地块种了相同的品种].

这样的安排称为一个**平衡不完全区组设计**(balanced incomplete block design,

BIBD). “区组” 是指种在各个农庄里的品种的集合. 说它们是 “不完全的” 是指每一个农庄并没有都种了所有的品种, [例如图 1 最左的一条边 —— 这是一个农庄 —— 就只种了 1 , 2 , 3 三种]. 然而这个试验是 “平衡的”, 因为每一对品种在各个农庄出现的数目是相同的 (现在是只出现 1 次). 这是一个 (7 , 3 , 1) 设计, 共有 7 个品种, 每个区块包含 3 个品种, 每一对品种若出现在一个区块里, 只出现 1 次. 它也是有限射影平面的例子. 因为它与几何学的联系, 所以品种也就叫做 “点”.

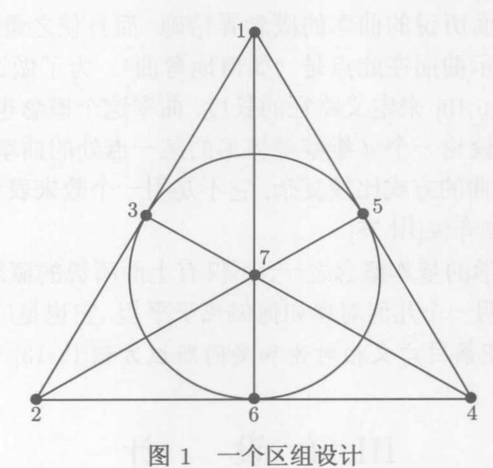


图 1 一个区组设计

数学家已经发展了关于 BIBD 和其他有关的设计类型的广泛理论. 事实上, 这种研究开始出现的时间比它们在统计学中的应用还要早. 1847 年, 寇克曼 (Thomas Penyngton Kirkman, 1806–1895, 英国数学家) 证明了: 一个 (v , 3 , 1) 试验当且仅当 $v \equiv 1$ 或 $3 \bmod 6$ 时存在 [这种试验现在称为一个施泰纳 (Jakob Steiner, 1796–1863, 瑞士数学家) 三元组, 虽然他到 1853 年才提出了存在性问题].

寇克曼还提出过一个较难的问题, 用他自己的话来说, 就是

> 十五个中学女学生一连七天每天出去散步都是三人一排, 要求每天的排队, 使得没有两个女生会两次同排一列.①

①这就是著名的寇克曼女生问题. 当时只是作为 “休闲数学” 的问题征解, 但是参加的人不少, 例如英国的大数学家凯莱、西尔威斯特都在内. 寇克曼自己给出的解如下 (英文字母代表着 15 个女生):

周日		ABC		DEF		GHI		JKL		MNO	
周一		ADH		BEK		CIO		FLN		GJM	
周二		AEM		BHN		CGK		DIL		FJO	⟵
周三	⟵	AFI	⟵	BLO	⟵	CHJ	⟵	DKM		EGN	
周四		AGL		BDJ		CFM		EHO		IKN	
周五		AJN		BIM		CEL		DOG		FHK	
周六		AKO		BFG		CDN		EIJ		HLM	

—— 中译本注

这个解答需要一个 (15 , 3 , 1) 施泰纳三元组, [15 个品种, 即 15 个女生; 每个区组就是去散步的一排女生, 包含 3 个女生 (品种); 每一对女生只能同排一次], 还有一个附加的要求, 就是 35 个区组 [每天出去 5 排女生, 共 7 天, 所以区组总数是 35] 要分成 7 个集合, 成为 7 个 "复本", 而每一个复本, 就是每天出去的 5 个区组, 要构成 35 个点的集合的一个分割, [就是所有的女生都得每天出去散步]. 寇克曼当时就给出了一个解, 但是直到 1960 年 Rau-Chauduri 和威尔逊 (Richard Wilson) 才证明了满足这个条件的 $(v\,,\,3\,,\,1)$ 设计当且仅当 $v \equiv 3 \bmod 6$ 时才有解.

对哪些 v , k , λ 才存在这样的设计? 用穷举法可以证明, 给定了 k , λ 后, 只有限制在某些同余类中, 这种 $(v\,,\,k\,,\,\lambda)$ 试验才存在 (我们在上面已经指出, 一个 $(v\,,\,3\,,\,1)$ 试验当且仅当 $v \equiv 1$ 或 $3 \bmod 6$ 时才存在). 威尔逊发展了一种渐近的存在理论, 证明了对于每一组 k , λ, 这种必要条件除了有限多个例外, 也是试验存在的充分条件.

设计的概念已经有了进一步的推广. 一个 t-$(v\,,\,k\,,\lambda)$ 设计具有如下的性质: 任意 t 个点包含在恰好 λ 个区组中. Luc Teirlinck 证明了对于任意的 t 都有非平凡的 t 设计存在. 但是, 当 $t > 3$ 时, 这种例子是很少见的.

统计学家的观点却稍有不同. 在开始的例子中, 如果只有 6 个农庄, 就不能用 BIBD 作试验了, 但是可以找可能最 "有效的" 设计 (即允许从试验结果中获得最多信息的试验). 如果 BIBD 存在, 它就是最有效的, 但在其他情况, 我们所知甚少.

还有其他类型的设计, 这些设计可能对于统计学很重要, 而且也引导到新的数学. 举一个例子, 下面是一个正交阵列 (orthogonal array), 如果取这个矩阵的任意两行, 而得出一个 2×9 矩阵, 则从 (0 , 1 , 2) 中任取两个符号所成的有序对都恰好作为一列出现在其中:

$$\begin{matrix} 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \\ 0 & 1 & 2 & 1 & 2 & 0 & 2 & 0 & 1 \\ 0 & 2 & 1 & 1 & 0 & 2 & 2 & 1 & 0 \end{matrix}$$

如果我们有 4 个不同的处理, 每一个都可以在 3 个不同水平上来实施, 而又有 9 个地块供试验之用, 就可以利用这种设计.

设计理论与其他组合学的主题, 如纠错码, 有密切的关系. 事实上, 费希尔 (Sir Ronald Aylmer Fisher, 1890–1962, 英国统计学家、进化生物学家和遗传学家) 在汉明 (Richard Wesley Hamming, 1915–1998, 美国数学家, 在计算机科学和通讯方面有重大贡献) 发现以他命名的纠错码前 5 年, 就作为一个设计 "发现" 了它. 其他有关的问题还有填充与覆盖问题, 特别是有限几何学, 许多经典的几何学的有限版本都可以看成是设计.

III.15 行 列 式
(Determinants)

2×2 矩阵

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

的行列式定义为 $ad-bc$. 3×3 矩阵

$$\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}$$

的行列式定义为 $aei+bfg+cdh-afh-bdi-ceg$. 这些表达式有什么共同之点, 怎样推广, 为什么这种推广有意义?

我们从第一个问题开始, 先作一些简单的观察. 这两个式子都是矩阵的元的乘积之和与差, 每一项都包含了矩阵的每一行和每一列的恰好一个元. 符号似乎总是附加在矩阵向上倾而不是向下倾的一排元素的乘积上.

当 $n\geqslant 4$ 时, 到一定程度为止, 把这个定义推广到 $n\times n$ 的矩阵上也是容易的. 我们只要取所有的由矩阵的 n 个元所成的乘积, 但这 n 个元, 必须每一行都有一个元, 每一列也都有一个元, 然后把它们求和或者求差. 难就难在哪些乘积要加起来, 哪些乘积要减去. 为了做这件事, 取一个乘积, 然后用它来定义集合 $\{1\ ,\ 2\ ,\cdots\ ,\ n\}$ 的一个排列 σ 如下: 对于每一个 $i\leqslant n$, 乘积中恰好含有来自第 i 行的一个元, 如果此元属于第 j 列, 就定义 $\sigma(i)=j$. 如果这个排列是偶排列, 对这个乘积就附上加号, 而把它加上; 如果是奇排列, 就附上负号, 而把它减去 (见条目置换群[III.68]). 这样, 作为一个例子, 我们来看上面的 3×3 行列式中的 afh 这一项. 相应的排列是把 1 变到 1, 把 2 变到 3, 又把 3 变到 2, 这是一个奇排列. 所以, 这一项得到的是一个负号.

我们还要解释一下, 为什么乘积的这种特殊的选择和上面定义的负号的取法很重要. 理由在于它多少告诉了我们, 如果把矩阵看成一个线性变换会有什么效果. 令 A 为一个 $n\times n$ 矩阵. 则我们在 [I.3 §3.2] 中解释过, A 确定了一个由 $\mathbf{R}^n$ 到 $\mathbf{R}^n$ 的线性映射 α. A 的行列式则告诉我们这个映射对于体积做了些什么事. 更精确地说, 若 X 为 $\mathbf{R}^n$ 的一个子集合, 其体积为 V, 则 αX 即用 α 对 X 作变换的结果, 其体积应该是用 A 的行列式去乘 V. 把这个结果用符号写成

$$\mathrm{vol}\,(\alpha X)=\det A\cdot \mathrm{vol}\,(X)\,.$$

例如考虑 2×2 矩阵

$$A=\begin{pmatrix}\cos\theta & -\sin\theta\\ \sin\theta & \cos\theta\end{pmatrix}.$$

相应的线性变换是 $\mathbf{R}^2$ 中旋转一个角 θ. 因为把一个图形作旋转, 不会改变其体积, 我们会期望其行列式等于 1, 所以肯定 [$\sin\theta\cdot(-\sin\theta)$ 这一项一定加负号, 这样会得到]$\cos^2\theta+\sin^2\theta=1$, 这就是毕达哥拉斯定理.

以上的解释在一个方面有点过分简单化: 行列式可以取负值, 而体积不会. 如果一个矩阵的行列式为 -2, 就表示这个线性变换既把体积大小增加 2 倍, 又把 "里面翻到外面" 作了一次反射.

当知道了行列式用体积的解释以后, 行列式的许多有用的性质就变得很显然了 (然而, 这个体积解释本身的正确性却不那么明显了; 要建立行列式的理论, 需要在别处下功夫). 下面给出三个这样的性质.

(i) 令 V 为一个向量空间[I.3 §2.3], 而 $\alpha:V\to V$ 为一线性映射. 令 $v_1,\cdots,v_n$ 为 V 的一个基底, 而 A 为 α 关于这个基底的矩阵. 现在再令 $w_1,\cdots,w_n$ 为 V 的另一个基底, 而 B 为 α 关于这另一个基底的矩阵. 于是 A 和 B 将是不同的矩阵, 但是因为它们代表同一个线性映射 α, 它们对于体积将产生同样的效果. 由此可知, $\det(A)=\det(B)$. 换一个方法来说, 行列式是线性映射的性质, 而不说它是矩阵的性质.

两个代表同样线性映射的矩阵称为是**相似的**. 可以证明, 当且仅当存在一个可逆矩阵 P 使得 $P^{-1}AP=B$ 时, A 和 B 为相似 (对于一个 $n\times n$ 矩阵 P, 如果存在一个矩阵 Q 使得 PQ 等于 $n\times n$ 恒等矩阵 I_n, 就有 P 为**可逆**, 由此还可以得到 QP 也等于 I_n. 如果这一点成立, 则称 Q 为 P 的**逆矩阵**, 并记为 P^{-1}). 我们刚才所证明的就是相似矩阵有相同行列式.

(ii) 若 A 和 B 为两个 $n\times n$ 矩阵, 并分别代表 $\mathbf{R}^n$ 的线性映射 α 和 β. 乘积 AB 就代表线性映射 $\alpha\beta$, 就是作了 β 再继之以 α 的线性映射. 因为作 β 已经对体积乘上了 $\det B$, 再作 α 又乘上 $\det A$, 所以, 作线性映射 $\alpha\beta$ 就会把体积乘上了 $\det A\cdot\det B$. 由此可得 $\det(AB)=\det A\cdot\det B$(即乘积的行列式等于行列式的乘积).

(iii) 若 A 是一个行列式为 0 的矩阵, 而 B 是另一矩阵, 则由上面讨论的行列式的乘积性质, AB 的行列式也为 0. 由此 AB 不可能等于 I_n, 因为 I_n 的行列式等于 1. 所以, 一个行列式为 0 的矩阵不会是可逆矩阵. 这个命题的逆也是成立的: 一个行列式不为 0 的矩阵一定是可逆的. 所以, 行列式给了我们一个矩阵是否可逆的判据.

III.16　微分形式和积分

(Differential Forms and Integration)

陶哲轩 (Terence Tao)

无需多说, 积分是单变量微积分的基本概念之一. 然而在这个主题里面出现了**三种积分概念: 不定积分** $\int f$ (也称反导数)、**无符号的定积分** $\int_{[a,b]} f(x)\,\mathrm{d}x$ (用来计算曲线下方的面积, 或者是具有变密度的 1 维物体的质量), 还有**有符号的定积分** $\int_a^b f(x)\,\mathrm{d}x$(用来计算例如使点从 a 运动到 b 时所需的功). 为简单起见, 在此限于 $f:\mathbf{R}\to\mathbf{R}$ 在整个实数直线上为连续的情况 (类似地, 在考虑微分形式时, 限于只讨论在整个区域上连续的情况). 我们也将非形式地使用 "无穷小量" 这样的术语以避免不得不讨论 (常规的)"ε-δ" 这样的分析问题, 而那是想要解决这些分析问题并使积分概念完全严格所不可少的.

在单变量微积分中的这三种积分之间当然互相有密切的关系, 事实上, *积分的基本定理*[I.3 §5.5] 就把有符号的定积分 $\int_a^b f(x)\,\mathrm{d}x$ 和一个不定积分 $F=\int f$ 用下式连接起来:

$$\int_a^b f(x)\,\mathrm{d}x = F(b)-F(a), \tag{1}$$

而有符号的与无符号的定积分之间, 又有下面的简单的恒等式成立:

$$\int_a^b f(x)\,\mathrm{d}x = -\int_b^a f(x)\,\mathrm{d}x = \int_{[a,b]} f(x)\,\mathrm{d}x\,, \tag{2}$$

此式适用于 $a\leqslant b$ 的情况.

然而, 当从单变量微积分转移到多变量微积分时, 这三种积分就开始明显地互相分别开来了. 不定积分被推广为**微分方程的解**, 或者一个连络、一个*向量场*[IV.6 §5], 或一个*丛*[IV.6 §5] 的**积分**. 无符号的定积分推广为*勒贝格积分*[III.55], 或者更一般地推广为一个**测度空间上的积分**. 最后, 有符号的定积分则推广为**微分形式的积分**, 而这就是本文所集中关注之处. 尽管这三个概念仍然互相关联, 但不如在单变量背景下那样可以互换地使用了. 微分形式的积分这个概念在微分拓扑、几何和物理学中具有基本的重要性, 而且提供了*上同调*[IV.6 §4] 的最重要的例子, 即德拉姆 (de Rham) **上同调**, (粗略地说) 德拉姆上同调正是量度了微积分的基本定理在高维情况和一般流形上失效的程度.

为了给这个概念提供一些启发, 我们非形式地重温一下有符号的定积分在物理学中的一个基本的应用, 就是在有外力的情况下, 计算把一个在一维空间 (设为 $\mathbf{R}$)

中运动的粒子, 从 a 点移动到 b 点所需的功 (例如把一个荷电的粒子在电场中移动). 在无穷小水平上, 把一个粒子从 $x_i \in \mathbf{R}$ 移动到邻近的点 $x_{i+1} \in \mathbf{R}$ 所需的功正比于位移 $\Delta x_i = x_{i+1} - x_i$, 而比例常数依赖于粒子的初始位置 x_i 处的外场 $f(x_i)$([它可能代表作用于粒子上的力或电场的力], 以上都允许小的误差). 所以这一小段的移动所需的功近似地是 $f(x_i)\,\Delta x_i$. 注意, 并没有要求 x_{i+1} 在 x_i 右方, 所以位移 Δx_i(以及无穷小功 $f(x_i)\,\Delta x_i$) 可能是负的. 回到计算从 a 移动到 b 所需的功这个非无穷小问题, 选择从 a 到 b 的任意的离散的路径 $x_0 = a, x_1, x_2, \cdots, x_n = b$, 并且用

$$\int_a^b f(x)\,\mathrm{d}x \approx \sum_{i=0}^{n-1} f(x_i)\,\Delta x_i \tag{3}$$

来逼近总功. 我们又一次不要求 x_{i+1} 位于 x_i 的右方. 很可能这条路径是反复地来来回回的, 例如可能对某一个 i 有 $x_i < x_{i+1} > x_{i+2}$. 然而, 结果是这种来回的效果最后互相抵消了. 不论选择何种路径, 当最大步长趋于零时, 上面的表达式 (3) 是收敛的, 其极限

$$\int_a^b f(x)\,\mathrm{d}x \tag{4}$$

就是一个有符号的定积分, 只要路径的总长度 $\sum_{i=0}^{n-1} |\Delta x_i|$(它控制了来回的总量) 有界. 特别是若 $a = b$ 而所有的路径都是封闭的 (即 $x_0 = x_n$), 我们看到, 有符号的定积分为零:

$$\int_a^b f(x)\,\mathrm{d}x = 0\,. \tag{5}$$

从有符号的定积分的这个非形式的定义, 很明显有**分段**(concatenation)**公式**

$$\int_a^b f(x)\,\mathrm{d}x = \int_a^c f(x)\,\mathrm{d}x + \int_c^b f(x)\,\mathrm{d}x \tag{6}$$

成立, 而不问 a, b 和 c 的相对位置如何. 特别有 (令 $a = c$ 并应用式 (5))

$$\int_a^b f(x)\,\mathrm{d}x = -\int_b^a f(x)\,\mathrm{d}x\,.$$

这样, 如果把由 a 到 b 的路径反过来变成由 b 到 a 的路径, 积分就会变号. 这一点与**无符号的定积分** $\int_{[a,b]} f(x)\,\mathrm{d}x$ 成为对比, 因为 a, b 之间的数的集合和 b, a 之间的数的集合完全一样. 这样, 我们看到路径和集合并不完全是一回事: 路径具有**定向**, 可以反转, 而集合则没有定向.

现在从一维积分转到高维积分, 即从单变量微积分转到多变量微积分. 结果是两个对象的维数都可以增加, 一是"包含空间"①, 现在取它为 $\mathbf{R}^n$, 而不再是 $\mathbf{R}$; 二是路径现在将要被一个有定向的 k 维流形 S 所取代, 就是在 S 上作积分. 例如, 如果 $n=3$, $k=2$, 就是在位于 $\mathbf{R}^3$ 内的一个曲面上积分.

先从 $n \geqslant 1$ 而 $k=1$ 的情况开始. 在此, 将在 $\mathbf{R}^n$ 中的一条连续可微的路径 (亦即一条**有向的可求长曲线**)γ 上积分, 起点和终点分别为 a 和 b(这两个点可以相同, 也可以不同, 视路径为开的或者为封闭的而定). 从物理的观点来看, 我们仍然是在计算将此点从 a 移动到 b 所需的功, 但是现在是在高维的空间中运动. 在一维情况下, 不必确定地指出沿哪条路径从 a 移动到 b, 因为所有的来回折转都会互相抵消, 而在高维情况下, 确切地选择路径 γ 就很重要了.

正式地说, 一条从 a 到 b 的连续可微的路径可以用一个定义在区间 $[0,1]$ 上的连续可微函数 γ 来描述, 这里 $\gamma(0)=a$, $\gamma(1)=b$ (这也称为用函数 γ 把这条路径**参数化**). 例如从 a 到 b 的直线段可以参数化为 $\gamma(t)=(1-t)\,a+tb$. 这个线段还有其他的参数化, 例如 $\tilde{\gamma}(t)=\left(1-t^2\right)a+t^2 b$. 然而, 和一维情况一样, 参数化的确切的选择, 最终并不影响积分. 但是, 把路径反转, 例如线段 $(-\gamma)(t)=ta+(1-t)\,b$ 就真正成了另一条从 b 到 a 的路径, 这是与 γ 不同的路径了. 沿 $-\gamma$ 的积分与沿 γ 的积分恰好反号.

和一维情况一样, 我们需要用离散的路径

$$x_0=\gamma(t_0)\ ,\ x_1=\gamma(t_1)\ ,\ x_2=\gamma(t_2)\ ,\cdots,\ x_n=\gamma(t_n)$$

来逼近 γ, 这里 $\gamma(t_0)=a$, $\gamma(t_n)=b$.② 在这里又一次允许折转, t_{i+1} 不必大于 t_i. 从 x_i 到 x_{i+1} 的位移 $\Delta x_i = x_{i+1}-x_i \in \mathbf{R}^n$ 现在是 $\mathbf{R}^n$ 中的**向量**而不再是标量 (事实上, 兼顾到以后推广到流形, 应该说 Δx_i 是包含空间 $\mathbf{R}^n$ 在 x_i 点的一个**无穷小切向量**). 在一维情况下, 把标量位移 Δx_i 转变为一个新数 $f(x_i)\Delta x_i$, 它与原来的位移成正比, 而比例常数为依赖于位置 x_i 的 $f(x_i)$. 在高维情况, 仍然有一个线性依赖关系, 但是, 因为现在位移成了向量, 就必须把比例常数代以由 $\mathbf{R}^n$ 到 $\mathbf{R}$ 的**线性变换** ω_{x_i}, 这样 $\omega_{x_i}(\Delta x_i)$ 就表示由 x_i 移动到 x_{i+1} 所需要的无穷小"功". 用技术术语来说, 这个功就是 x_i 处的切空间上的**线性泛函**, 也就是 x_i 处的**余切向量**. 类比于 (3), 从 a 到 b 的净功 $\int_\gamma \omega$ 有以下的逼近:

$$\int_\gamma \omega \approx \sum_{i=0}^{n-1} \omega_{x_i}(\Delta x_i)\ . \tag{7}$$

①为简单计, 从欧几里得空间 $\mathbf{R}^n$ 上的积分开始, 虽然, 如果从更一般的空间 (例如 n 维流形) 开始, 微分形式的积分这个概念的真正力量将会看得更加明显.

②这里原书有一个排印错误, 把 t_n 误为 t_1 了. —— 中译本注

也和一维情况一样可以证明, 当最大步长 $\sup_{0\leqslant i\leqslant n-1}|\Delta x_i|$ 趋于零而路径总长保持有界时, (7) 式的右方收敛. 极限记作 $\int_\gamma \omega$ (请记住, 我们是限于连续函数的, 而极限的存在就需要 ω 的连续性).

ω 是一个新的对象. 它对 $\mathbf{R}^n$ 中的每一点都指定了一个余切向量, 就称 ω 为一个 **1-形式**, 而 (7) 式就告诉我们如何在路径 γ 上求 1-形式 ω 的积分. 这个式子把重点稍微转移了一点: 用 "路径"γ 来 "积"ω 这个 1-形式, [也就是逐渐把 "积分区域 γ" 与 "被积表达式 ω" 放在同等重要的位置上]. 说真的, 把积分想成一个**二元运算**(多少像是 "点积" 即内积一样) 是很有用的: 它以曲线 (即路径)γ 和 1-形式 ω 为输入, 而输出一个标量 $\int_\gamma \omega$. 事实上, 在曲线与 1-形式之间有一种 "对偶性". 例如比较下面两个恒等式: 一个是表示 1-形式的积分是一个线性运算这一基本事实 (的一部分) 的恒等式

$$\int_\gamma (\omega_1+\omega_2)=\int_\gamma \omega_1+\int_\gamma \omega_2,$$

另一个是 (6) 式的推广

$$\int_{\gamma_1+\gamma_2}\omega=\int_{\gamma_1}\omega+\int_{\gamma_2}\omega,$$

这里 γ_1 的终点就是 γ_2 的起点, 从而 γ_1 和 γ_2 就是 $\gamma_1+\gamma_2$ 的分段 (concatenation)[①].

回忆一下, 如果 f 是一个从 $\mathbf{R}^n$ 到 $\mathbf{R}$ 的连续可微函数, 则它在 x 点的导数就是一个从 $\mathbf{R}^n$ 到 $\mathbf{R}$ 的线性映射 (见 [I.3 §5.3]), 如果 f 是连续可微的, 则这个线性映射连续依赖于 x, 所以可以看作一个 1-形式, 记为 $\mathrm{d}f$, 并且把 x 点的这个连续映射写为 $\mathrm{d}f_x$. 这个 1-形式可以刻画为唯一的对于所有无穷小 v 都给出逼近式[②]

$$f(x+v)\approx f(x)+\mathrm{d}f_x(v)$$

的 1-形式 (严格地说, 这个逼近是唯一的满足以下条件的 1-形式: 当 $v\to 0$ 时, $|f(x+v)-f(x)-\mathrm{d}f_x(v)|/|v|\to 0$).

微积分的基本定理现在推广为

$$\int_\gamma \mathrm{d}f=f(b)-f(a), \tag{8}$$

这里只要求 γ 是从点 a 到点 b 的有向路径. 特别是如果 γ 是封闭的, 则 $\int_\gamma \mathrm{d}f=0$. 注意, 在理解 (8) 式左方时, 我们是把它作为 $\int_\gamma \omega$ 的一个特例, 特别之处就在于 ω

① 这里的对偶性, 用同调和上同调的抽象的但是广泛得多的形式来理解最好. 特别是这样可以除去 γ_1 必须终止于 γ_2 的开始之处这一限制, 而把积分概念推广到不仅包括在一条路径上的积分, 而且还可以在路径的 "**形式和**" 与 "**形式差**" 上的积分, 这就使得曲线和 1-形式的对偶性更加对称.

②原书此处有印刷错误. —— 中译本注

现在恰好就是 $\mathrm{d}f$. 还要注意, 现在 $\mathrm{d}f$ 有了独立的意义, 哪怕它并不位于积分号下, 它是一个 1-形式.

一个 1-形式, 如果对于充分小[①]的封闭曲线积分为零, 就称为**闭形式**, 而如果有一个连续可微函数 f 存在, 使这个 1-形式恰好是 $\mathrm{d}f$, 就称它是**恰当的**. 所以, 基本定理 (8) 就意味着每一个恰当形式都是闭的. 这是一个一般的事实, 对于流形上的 1-形式也是成立的. 其逆是否为真, 即是否所有的闭形式都是恰当的? 如果区域是欧几里得空间, 或甚至是任意的**单连通流形**, 答案也是肯定的 (这是**庞加莱引理**的特例). 但是对于一般的区域, 它是不成立的. 用现代的术语来讲, 这种区域的德拉姆上同调可以是非平凡的.

我们已经看到, 一个 1- 形式可以看成一个对象 ω 对每一个路径 γ 赋以一个标量 $\int_\gamma \omega$. 当然, ω 并不是一个按照老概念的由路径到标量的一般的函数, 它还必须满足分段和反向的规律, 再加上我们对于连续性的要求, 或多或少地迫使我们把它与一个连续变动线性函数联系起来, 这个函数连同 γ 就可以定义一个积分. 现在让我们来考虑如何把这个基本思想从路径推广到 k 维集合上去, 这里 $k > 1$. 为简单起见, 我们坚持看 2 维情况, 就是考虑在 $\mathbf{R}^n$ 的 (有向的) 曲面上对微分形式积分, 因为这就已经说明了一般情况的许多特性.

从物理上说, 当考虑某一个场 (例如磁场) 穿过一个曲面的**流量**时, 这种积分就会出现. 在一维情况下, 我们是把 1 维有向曲线参数化为一个把区间 $[0, 1]$ 映入 $\mathbf{R}^n$ 的连续可微函数 γ 的, 所以很自然地会把 2 维有向曲面参数化为一个定义于 $[0, 1]^2$ 上的连续可微函数 ϕ. 这确实还没有概括所有我们想要在其上积分的曲面, 但是结果是可以把一般的曲面切成小片, 而每一片都可以用 $[0, 1]^2$ 这样的 "好" 区域来参数化.

在一维情况下, 把有向的区间 $[0, 1]$ 切成从 t_i 到 $t_{i+1} = t_i + \Delta t$ 的无穷小的有向区间, 而它们给出从 $x_i = \gamma(t_i)$ 到 $x_{i+1} = \gamma(t_{i+1}) = x_i + \Delta x_i$ 的无穷小曲线. 注意, Δx_i 和 Δt 之间由一种逼近关系联系起来 $\Delta x_i = \gamma'(t_i)\Delta t$[②]. 在 2 维情况下, 把单位正方形 $[0, 1]^2$ 以一种自然的方式分成许多无穷小正方形[③]. 取一个典型的无穷小正方形, 其四角为 (t_1, t_2), $(t_1 + \Delta t, t_2)$, $(t_1, t_2 + \Delta t)$, $(t_1 + \Delta t, t_2 + \Delta t)$.[前面我们已经说到用一个连续可微的函数 $\phi:\ [0, 1]^2 \to \mathbf{R}^n$ 来定义一个曲面, 在这个曲面的坐标表示 $x = \phi(t_1, t_2)$ 中, 把 $x \in \mathbf{R}^n$ 看成一个向量. 现在随着 $[0, 1]^2$ 被分成无穷小正方形], 曲面也被分成小块, 每一个小块有四个顶点: $\phi(t_1, t_2)$, $\phi(t_1 + \Delta t, t_2)$, $\phi(t_1, t_2 + \Delta t)$, $\phi(t_1 + \Delta t, t_2 + \Delta t)$, 而且这

① "充分小" 一词需要认真解释, 否则会引起误会. 所谓 "小" 的确切的解释是这个曲线应该是可收缩的(contractible), 即可以连续地形变收缩为一个点.

②原书为 Δx_i. —— 中译本注

③ 也可以用无穷小的有向的矩形、平行四边形、三角形等等, 这些都会引导到等价的积分定义.

些小块都附有定向. 因为 ϕ 是连续可微的, 在小的距离尺度下, 都可以用线性函数来逼近, 所以这个小块近似地就是 $\mathbf{R}^n$ 中的有向的平行四边形, 其四个顶点 (用向量来表示) 就是 x , $x+\Delta_1 x$,$x+\Delta_2 x$, $x+\Delta_1 x+\Delta_2 x$, 这里 $x=\phi(t_1\,,\,t_2)$, 而 $\Delta_1 x$, $\Delta_2 x$ 分别是无穷小向量

$$\Delta_1 x=\frac{\partial\varphi}{\partial t_1}(t_1\,,\,t_2)\,\Delta t\,,\quad \Delta_2 x=\frac{\partial\varphi}{\partial t_2}(t_1\,,\,t_2)\,.$$

我们把 $\mathbf{R}^n$ 中的这个对象称为**尺度**为 $\Delta_1 x\wedge\Delta_2 x$、**基点**为 x 的无穷小平行四边形. 我们暂时把 "$\wedge$" 这个符号只看成是一个方便的记号, 而不加解释. 为了模仿曲线的情况来作积分, 现在需要某种在基点 x 处的连续依赖于 x 的泛函 ω_x. 这个泛函应该把输入进去的平行四边形变成一个无穷小量 $\omega_x\,(\Delta_1 x\wedge\Delta_2 x)$ 输出, 而这个无穷小量就可以看成通过这个平行四边形的 "流量".

和一维情况一样, 应该要求 ω_x 具有某些性质. 例如, 如果把 $\Delta_1 x$ 加倍, 也就是把平行四边形的一边加了一倍, (根据 ω 的连续性) 过此平行四边形的 "流量" 也会加倍. 一般地说, $\omega_x\,(\Delta_1 x\wedge\Delta_2 x)$ 对于每一个向量 $\Delta_1 x$ 和 $\Delta_2 x$ 都是线性的, 或者说, 它是**双线性的**(这一点推广了一维情况的线性依赖性).

另一个重要性质是

$$\omega_x\,(\Delta_2 x\wedge\Delta_1 x)=-\omega_x\,(\Delta_1 x\wedge\Delta_2 x)\,. \tag{9}$$

就是说, 双线性形式 ω_x 是**反对称的**. 这件事也有一个直观的解释：除了定向相反以外, 由 $\Delta_1 x\wedge\Delta_2 x$ 来表示的平行四边形和由 $\Delta_2 x\wedge\Delta_1 x$ 所表示的平行四边形是完全一样的, 所以通过后者的流量现在应该反号来计算, 反过来也是一样. 看出这一点还有另一个方法, 就是注意到, 如果 $\Delta_1 x=\Delta_2 x$, 则平行四边形 [因为两邻边重合] 而退化 [为过基点 x 的线段], 从而流量成为零：$[\omega_x\,(\Delta_1 x\wedge\Delta_1 x)=0]$. 由此以及双线性性质, 即可得出反对称性. **2-形式** ω 就是在每一点 x 指定一个 ω_x.

如果 ω 是一个 2- 形式, 而 ϕ 是一个连续可微函数, 则 "ϕ 上" 的积分 (准确一些, 应该说是 "在有向正方形 $[0\,,\,1]^2$ 被 ϕ 映射的像上" 的积分 $\int_\varphi \omega$ 可以用积分和

$$\int_\phi \omega\approx\sum_i \omega_{x_i}\,(\Delta_1 x_i\wedge\Delta_2 x_i) \tag{10}$$

来逼近, 这里把 ϕ 的像划分为近似的基点在 x_i 处的平行四边形 $\Delta_1 x_i\wedge\Delta_2 x_i$). 我们不必去决定这些小平行四边形是如何排列的, 因为加法是可交换与结合的. 可以证明, 当平行四边形的划分 "越来越细" 时, (10) 右式必收敛于唯一极限, 但现在不来确切地讲这件事了.

至此, 我们已经说明了怎样在一个 2 维有向曲面上积分一个 2-形式. 可以更一般地定义一个 n 维流形 (例如 $\mathbf{R}^n$) 上的 k-形式, 这里 $0 \leqslant k \leqslant n$, 并且在这个流形的 k 维曲面上来积分这个 k-形式. 举例来说, 流形 X 上的一个 0-形式就是其上的标量函数: $f \to \mathbf{R}$, 它在正定向的点 x 处的积分就是 $f(x)$, 而在负定向的点 x 处的积分则是 $-f(x)$. 一个 k-形式告诉我们怎样对一个尺度为 $\Delta x_1 \wedge \cdots \wedge \Delta x_k$ 的无穷小平行多面体 (parallelipiped) 指定一个值, 从而在一个 k 维 "曲面" 的一部分上指定一个值, [然后再定义 k-形式在此流形的一个 k 维 "曲面" 上的积分], 完全类似于我们已经见到了的 2 维情况下的作法. 再作一个规定: 如果 $k \neq k'$, 则规定 k-形式在一个 k' 维流形上的积分为零. 把 0-形式、1-形式、2-形式等等 (以及它们的形式和与差) 统称为**微分形式**.

对于标量函数, 可以作三个基本的运算: 加法 $(f, g) \mapsto f+g$、乘法 $(f,g) \mapsto fg$, 还有微分 $f \mapsto \mathrm{d}f$. 最后这个运算只有当 f 连续可微时才有意义, 所以不是那么基本. 这些运算之间有不同的相互关系. 例如乘积对于加法是分配的,

$$f(g+h) = fg + fh\ .$$

微分对于乘法是一个 "**导运算**"[①],

$$\mathrm{d}(fg) = (\mathrm{d}f)\, g + f\,(\mathrm{d}g)\ .$$

这三个运算都可以推广到微分形式 [及其积分]. 加法很容易, 如果 ω 和 η 是两个 k-形式, 而 $\phi : [0, 1]^k \to \mathbb{R}^n$ 是一个连续可微函数, 则定义 $\int_\phi (\omega+\eta) = \int_\phi \omega + \int_\phi \eta$. 微分形式的乘法是**外积** $\wedge$(或称**楔积**), 它的定义粗略地说就是: 如果 ω 是一个 k-形式, 而 η 是一个 l-形式, 则定义 $\omega \wedge \eta$ 为一个 $(k+l)$-形式, 而对一个 $k+l$ 维的以 x 为基点尺度为 $\Delta x_1 \wedge \cdots \wedge \Delta x_{k+l}$ 的无穷小平行多面体, 分别取 ω 和 η 对基点为 x, 尺度分别为 $\Delta x_1 \wedge \cdots \wedge \Delta x_k$ 以及 $\Delta x_{k+1} \wedge \cdots \wedge \Delta x_{k+l}$ 的无穷小平行多面体所指定的值相乘.

至于微分, 若 ω 是一个连续可微的 k-形式, 则其微分 $\mathrm{d}\omega$ 是一个 $(k+1)$-形式, 它在某种意义下度量 ω 的 "变化率". 为了看清这是什么意思, 特别是看清为什么 $\mathrm{d}\omega$ 是一个 $(k+1)$ -形式, 考虑可以怎样来回答下面一类的问题. 设给定了一个 $\mathbf{R}^3$ 中的球面和一个流, 而我们想知道通过这个球面的净流量, 就是流入的量与流出的量之差. 解决这个问题的方法是: 一方面用许多小平行四边形之并去逼近球面, 再考虑通过每一个平行四边形的流量, 并把它们加起来, [这个流量就大小而言, 是一

① 原书在这里用了 derivative 一词, 这当然是对的. 但是这个英文字容易与 "导数" 混淆, 实际上在这里并不是指的导数, 而是指导数的莱布尼兹法则. 但是具有这种形式性质的对象很多, 所以许多文献上称它为 "莱布尼兹性质". 因此这里我们译为 "导运算". —— 中译本注

个 2-形式 “乘” 上此平行四边形的面积, 其方向由此平行四边形的定向决定]. 另一方面用许多小平行六面体之并去逼近球体, 考虑流出每一个平行六面体的**净流量**, 再把它们加起来. 如果这个平行六面体充分小, 则为了逼近一个平行六面体的净流量, 可以取每一个方向的一对边缘, [它们都是平行四边形], 并且研究通过这两个边缘的流量之差, 就是从一个边缘流出的流量减去从对着它的边缘流入的流量, [把从 3 个方向的边缘所得的这个差加起来], 自然就度量了这个 2-形式的变化.

把这些净流量相加的过程可以比较严格地用一个 3-形式在球体上的积分来描述. 这样, 我们就可以很自然地期望, 关于 2-形式的变化的信息包含在一个 3-形式中.

这些运算的具体构造需要一点代数, 在此略去. 然而, 我们要提醒, 它们服从与标量的对应运算很相似的规则, 但有一点不同, 就是符号上会有些变化, 而归根结底, 这些变化来自反对称性 (9). 例如, 如果 ω 是一个 k-形式, 而 η 是一个 l-形式, 则乘法的交换律就成了

$$\omega \wedge \eta = (-1)^{kl}\ \eta \wedge \omega\ ,$$

这基本上是由于交换一个 k- 形式和一个 l- 形式, 需要总共 kl 个对换; 导运算规则现在成了

$$\mathrm{d}\left(\omega \wedge \eta\right) = (\mathrm{d}\omega) \wedge \eta + (-1)^k\, \omega \wedge \mathrm{d}\eta\ .$$

微分算子 d 的另一个规则是幂零性质:

$$\mathrm{d}\left(\mathrm{d}\omega\right) = 0\ . \tag{11}$$

这一点看起来与直觉大相径庭, 但是却有基本的重要性. 为了看出为什么能够期望这种事情, 我们来想一想对于 1-形式微分两次会发生什么情况. 原来的 1-形式会对于每一个无穷小的直线段指定一个标量. 它的微分① 是一个 2-形式, 而对每一个无穷小平行四边形赋予一个标量. [前面讲到微分定义时, 已经说明微分与变化率的关系, 所以现在得到的标量] 本质上表示原来的 1-形式当绕行这个平行四边形的四边一周所得到的那些标量之和, 虽然如果想要得到一个有意义的结果还要除以这个平行四边形的面积. 如果再重复以上的运算, [即再作一次微分, 得到一个 3-形式, 而它赋予一个平行六面体以一个标量]. 按上面所说, 就会得到那个 2-形式对此平行六面体的边缘即构成边缘的六个平行四边形所赋予的标量之和, 而每一个这样的标量又是 1-形式赋予这个平行四边形的四边的标量之和. 这样一来, 那个平行六面体的每条棱都走了两次 (因为每条棱属于两个面), 而且方向相反. 所以每条棱对于总和的贡献都被抵消了, 而总和为零. [这就是 (11) 式的解释].

①原书用了 derivative, 但是在上面一个脚注里已经说了此字在本文中的意义, 所以在这里只好按通常的文献的说法改称微分.

上面讲到了球面上的一个 2-形式的积分及其微分 (这是一个 3-形式) 在球体上的积分的关系, 可以认为是微积分的基本定理的推广, 而它还可以极大地推广为**斯托克斯**(Sir George Gabriel Stokes, 1st Baronet, 1819–1903, 英国数学家)**定理**

$$\int_S \mathrm{d}\omega = \int_{\partial S} \omega\,, \tag{12}$$

它对任意的可定向流形 S 和任意微分形式 ω 都成立, 这里 ∂S 是 S 的有向边缘 (这个概念现在不来定义了). 事实上, 这个定理可以认为就是导运算 $\omega \mapsto \mathrm{d}\omega$ 的定义, 所以微分算子 d 是边缘算子 ∂(就是把一个流形变为其边缘这个算子) 的**伴算子**(举例来说, 恒等式 (11) 对偶于以下的几何事实: 一个有向流形 S 的边缘 ∂S 本身没有边缘: $\partial(\partial S) = \varnothing$). 斯托克斯定理的特例是: 当 S 是一个闭流形 (即没有边缘的流形) 时 $\int_S \mathrm{d}\omega = 0$. 看到这一点, 就使我们能够把闭形式和恰当形式的概念推广到一般的微分形式, (再加上式 (11)) 就允许我们完整地建立起德拉姆**上同调.**

我们已经看到, 0-形式可以和标量函数等同起来. 同样, 在欧几里得空间中, 可以利用内积把 1-形式与向量场等同起来. 而在特殊的 (但是在物理上非常有用的)3 维欧几里得空间 $\mathbf{R}^3$ 里, 2-形式也能通过有名的**右手法则**①与向量场等同起来, 而用这个法则的变体, 还可以把 3-形式与标量函数等同起来 (这是所谓的霍奇**对偶性**的一个例子). 在 $\mathbf{R}^3$ 的情况下, 当 ω 是一个 0-形式 f 时, 微分算子 d 就与**梯度算子**$f \mapsto \nabla f = \operatorname{grad} f$ 等同起来; 当 ω 是一个 1-形式 (即向量场)X 时, 微分算子 d 则与**旋度算子**$X \mapsto \nabla \times X = \operatorname{curl} X$ 等同起来; 而当 ω 是一个 2-形式 X 时 ([注意, 2-形式已经与向量场等同起来了, 所以仍用记号 X]) 微分算子 d 则变成了所谓**散度算子**$X \mapsto \nabla \cdot X = \operatorname{div} X$**.** 这样, (11) 式就变成了下面两个式子: 对于一切光滑的标量函数, $\nabla \times \nabla f = 0$, 以及对于一切光滑的向量场, $\nabla \cdot (\nabla \times X) = 0$②. 在这个解释下, 斯托克斯定理就成了关于线积分和面积分的定理, 而在多元微积分教程中, 分别称为 “散度定理”“格林定理” 和 “斯托克斯定理” 等等.

正如有符号的定积分与无符号的定积分是由式 (2) 互相连接一样, 微分形式的积分与勒贝格积分 (或黎曼积分) 之间也有联系. 在欧几里得空间 $\mathbf{R}^n$ 上, 有 n 个坐标函数 $x_1, x_2, \cdots, x_n : \mathbf{R}^n \to \mathbf{R}$. 它们的微分都是 $\mathbf{R}^n$ 上的 1-形式. 取它们的外积, 就可以得出一个 n-形式 $\mathrm{d}x_1 \wedge \cdots \wedge \mathrm{d}x_n$. 可以用任意的 (连续) 标量函数 $f : \mathbf{R}^n \to \mathbf{R}$ 去乘它, 而得到另一个 n- 形式 $f(x)\,\mathrm{d}x_1 \wedge \cdots \wedge \mathrm{d}x_n$. 如果 Ω 是 $\mathbf{R}^n$ 中的任意有界开集合, 有恒等式

$$\int_\Omega f(x)\,\mathrm{d}x_1 \wedge \cdots \wedge \mathrm{d}x_n = \int_\Omega f(x)\,\mathrm{d}x\,,$$

①这是一个完全人为的规定, 用左手法则也很容易实现这种等同性, 而除了不时需要对符号做一些无害的变动以外, 我们仍可推导出本质相同的理论.

②原书漏了等式的 “右方 = 0”. —— 中译本注

式左是一个微分形式在 Ω(看作一个有正定向的 n 维流形) 上的积分, 而式右则是 Ω 上的函数 f 的勒贝格或黎曼积分. 如果赋 Ω 以负定向, 则左方应该改变符号. 这个对应关系就是式 (2) 的推广.

在形式上还有最后一个运算值得提到. 设有从一个流形 X 到另一个流形 Y 的连续可微映射 $\Phi: X \to Y$(这里 X 和 Y 的维数允许不同). 这时, 当然每一点 $x \in X$ 都被**推前**为 Y 中的一点 $\Phi(x)$. 类似地, 令 $v \in T_x X$ 为基点在 x 的 X 的切向量, 它也会被**推前**为 Y 的基点在 $\Phi(x)$①的切向量 $\Phi_* v \in T_{\Phi(x)}(Y)$. 非形式地说, $\Phi_* v$ 可以用无穷小逼近 $\Phi(x+v) = \Phi(x) + \Phi_* v$ 来定义. 我们可以把 $\Phi_* v$ 写成 $\Phi_* v = D\Phi(x) v$, 这里

$$D\Phi: T_x X \to T_{\Phi(x)} Y$$

是多元映射 Φ 在 $\Phi(x)$ 点的**导映射**(derivative). 最后, 每一个 k 维有向流形 S 也推前为 Y②上的 k 维流形 $\Phi(S)$, 虽然当 Φ 的像的维数小于 k 而退化时这个推前的流形也就退化.

我们在前面看到积分是流形和微分形式之间的对偶配对, 因为在映射 $\Phi: X \to Y$ 下, 流形被推前了, 我们可以期望微分形式会被从 Y 到 X **拉回**. 事实上, 对于 Y 上的任意一个 k-形式 ω, 都可以定义其拉回为 X 上的唯一的使得下式成立的 k-形式 $\Phi^*\omega$, 这个式子就是

$$\int_{\Phi(S)} \omega = \int_S \Phi^* \omega .$$

这个式子其实就是变量变换公式, 因为在 0-形式 (即标量函数) 的情况, 标量函数 $f: Y \to \mathbf{R}$ 的拉回 $\Phi^* f: X \to \mathbf{R}$ 可以显式地由式 $\Phi^* f(x) = f(\varphi(x))$ 给出, 而 1-形式的拉回则可由下式显式地给出:

$$(\Phi^*\omega)_x(v) = \omega_{\phi(x)}(\Phi_* v).$$

对于其他的微分形式, 也可以给出类似的定义. 拉回算子有好几个 “很好的” 性质, 例如它保持外积和微分:

$$\Phi^*(\omega \wedge \eta) = (\Phi^*\omega) \wedge (\Phi^*\eta);$$
$$\mathrm{d}(\Phi^*\omega) = \Phi^*(\mathrm{d}\omega) .$$

利用这样一些性质, 可以毫不费力地恢复多元微积分的变量变换公式. 进一步, 可以毫不费力地把整个理论从欧几里得空间推广到其他流形. 正因为这个原因, 微分学和积分的理论是研究流形的不可少的工具, 特别是在*微分拓扑*[IV.7] 中.

①原书误为 $\Phi * x$. —— 中译本注
②原书误为 x. —— 中译本注

III.17 维
(Dimension)

2 维集合与 3 维集合有什么区别? 我们可能给出下面的粗略的回答: 2 维集合位于一个平面内, 而 3 维集合会填满空间的一部分. 这是一个好的回答吗? 对于许多集合似乎是的, 例如三角形、正方形、圆都可以画在一个平面上, 而四面体、立方体和球体就不行. 但是球体的表面即球面又如何? 通常都会认为球面是 2 维的, 而与球体是 3 维的相对照, 但是球面并不位于一个平面内.

这是否意味着我们的粗略的定义不正确? 不完全如此. 从线性代数的角度来看, 代表以 $\mathbf{R}^3$ 的原点为中心以 1 为半径的球面的集合 $\{(x, y, z): x^2+y^2+z^2=1\}$ 确实是 3 维的, 恰好是因为它并不位于一个平面内 (可以把这件事用代数语言表述为: 由球面生成的仿射子空间是整个 $\mathbf{R}^3$). 然而在这种意义下的 "3 维" 并没有充分考虑到一个不精确的思想: 球体的表面没有厚度. 是否肯定还有 "维" 的另一个定义, 使得球体的表面按照这个定义确实是 2 维的?

这个例子说明, 维这个概念虽然在整个数学中都很重要, 却不是一个单一的概念. 结果是有许多自然的方式来推广关于简单的集合如正方形、立方体的维的概念. 这些推广时常又是互不相容的, 就是说, 一个集合的维数是多少, 视采用的定义不同而有变化. 本文下面就要提出几种不同的定义.

我们关于集合的维数的第一个基本的思想是: "维数就是为了确定一个点所需的坐标的数目". 可以用这一点来论证, 关于球面的维数是 2 的直觉是有道理的: 只要给出球面上一点的经度和纬度就能确定这个点. 但是要把这个思想变成严格的数学定义还要费点事, 因为想要确定球面上的一个点, 只要**一个**数就够了, 如果不介意用非常矫揉做作的方式来完成这件事的话. 这是因为可以取任意两个数, 然后把它们的小数展开的各位数穿插起来成一个数. 例如从 $\pi=3.141592653\cdots$ 和 $\mathrm{e}=2.718281828\cdots$, 可以做出一个数 $32.17411852982168523 8\cdots$, 也可以从它跳着取各位数, 这就重新返回到 π 和 e 了. 甚至可以找到一个从闭区间 $[0, 1]$(即从 0 到 1 的一切实数包括 0 和 1 的集合) 到球面的连续函数 f, 使它能取每个值.

所以我们必须决定, 所谓 "自然的" 坐标系是什么意思. 做这个决定的方法之一, 会引导到流形的定义, 关于这个很重要的概念的讨论可见 [I.3 §6.9] 和条目*微分拓扑*[IV.7]. 这个方法基于以下的思想, 就是球面的每一点都包含在一个 "看起来" 像是平面的一部分的邻域 N 中, 所谓 "像" 是指在 N 和欧几里得平面 $\mathbf{R}^2$ 的一个子集之间, 存在一个很 "好" 的一一对应 ϕ. 在这里, "好" 也有不同的意义, 其中一个典型的意义是 ϕ 及其逆都是连续的、可微的, 甚至无限可微的.

像这样, d 维集合这个直觉的概念, 即需要 d 个数来确定一点的位置, 可以发展为严格的定义, 使得它能够如我们所期望的那样, 告诉我们球面确实是 2 维的. 现在我们来取另一个直觉的概念, 看一看从中能够得到些什么.

假设取一片纸, 并且把它切成两片. 分开这两片的边缘是一条曲线, 而在正常情况下, 我们会把曲线想成 1 维的. 为什么曲线是 1 维的呢? 我们可以用同样的推理: 把曲线切成两段, 则这两段相遇之处是一个点 (或者当此曲线是一个环时, 是两个点), 而点是零维的. 这样, 说一个集合是 d 维的还包含这样一个意思, 就是如果想把它一分为二, 就需要一个 $d-1$ 维集合.

让我们试着把这个思想讲得清楚一些. 设 X 为一集合而 x , y 为其中两点. 如果没有一条连接这两点而又避过 Y 的连续的路径, 就称 Y 为 x , y 间的**障碍**. 例如, 如果 X 是一个半径为 2 的球体, x 是球心, y 是 X 边缘上的一点, 则一个半径为 1 的同心球面就是 x , y 间可能的障碍. 有了这个术语, 就可以给出下面的归纳定义: 有限集合规定为 0 维的, 而一般地, 我们说 **X最多为 d 维**的, 如果 X 中的任意两点之间必有**最多为 $d-1$ 维的障碍**的话. 如果 X 最多是 d 维的, 但不是最多为 $d-1$ 维的, 就说 **X为 d 维**的.

上面的定义是有意义的, 但是它会有困难, 可以作出一个病态的集合 X 使之成为平面上任意两点的障碍, 但是其中又不包含任意的曲线段, 因此 X 成为 0 维的, 从而使平面成为 1 维的, 这当然不能令人满意. 把上面的定义稍作修改就可以消除这种病态, 而给出一个由布劳威尔[VI.75] 提出的如下的定义: 我们说一个完备的度量空间[III.56]X 最多是 d 维的, 是指对于任意两个互相分离的闭集合 A , B, 恒可找到两个互相分离的开集合 U 和 V 使得 $A\subset U$, $B\subset V$, 而 $U\cup V$ 的余集合 Y(即 X 中所有不在 $U\cup V$ 中的点所成的集合) 最多为 $d-1$ 维的. 集合 Y 是一个障碍, 而这里与前面主要的区别在于我们要求它为闭集合. 这个定义当然也是归纳的, 它从空集合为 -1 维集合开始. 布劳威尔的这个定义称为集合的**归纳维数**.

下面是另一个基本的思想, 导致由勒贝格[VI.72] 提出的维的有用的定义. 假设想要用较短的区间来覆盖一个开的实数区间 (就是一个区间但不包含两个端点), 这时不得不要求这些较短的区间互相重叠, 但是可以做到没有一个点属于两个以上的短区间, 只要在作新区间时让其靠近前一个区间的端点就行了.

现在假设想用较小的正方形去覆盖一个开正方形 (就是不包含边缘的正方形), 也不得不让这些小正方形互相重叠, 但是现在的情况还要更糟一点, 有些点会落在 3 个小正方形里面. 然而如果像砌砖一样来排列这些小正方形, [先如图 1 那样把这些小正方形紧靠着, 再把每一个小正方形都稍微放大一点], 就可以做出这样一个覆盖, 使得没有任何四个小正方形重叠在一起, [即有公共点]. 一般说来, 如果想要用小的开集合来覆盖一个典型的 d 维集合, 需要让 $d+1$ 个小的开集合重叠 [即有公共点], 但是不需让更多的小的开集合重叠了.

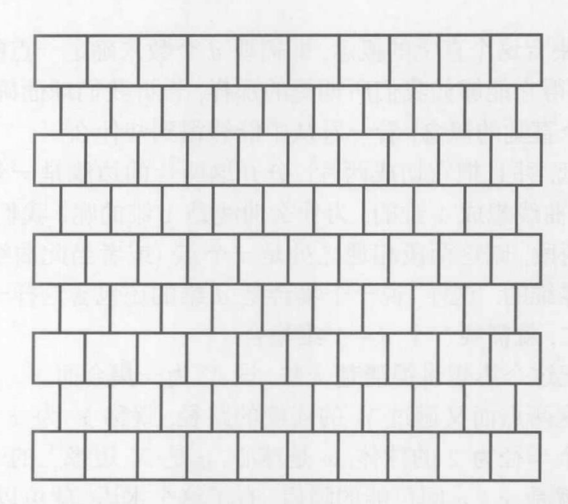


图 1 怎样用正方形作覆盖, 而任意四个小正方形都不重叠

这个做法所引导到的精确定义一般得惊人, 它不只对于 $\mathbf{R}^n$ 的子集合有意义, 而且甚至可用于一般的任意*拓扑空间*[III.90]. 我们说一个集合最多是 d 维的, 如果不论用什么样开集合的有限集合 $U_1, \cdots, U_n$ 去覆盖 X, 总可以找到另一个由开集合 $V_1, \cdots, V_m$ 组成的有限集合, 具有下面的性质:

(i) 这些集合 V_i 覆盖整个 X.

(ii) 每个 V_i 都至少是一个 U_j①的子集合.

(iii) 没有一个点含于多于 $d+1$ 个 V_i 中.

如果 X 是一个度量空间, 可以选择 U_i 具有小的直径, 这样迫使 V_i 也很小. 所以, 这个定义说的基本上就是可以用一组开集合 V_i 覆盖 X, 而使得 X 的每一点最多含于 $d+2$ 个 V_i 中, 而且这些开集合 V_i 可以取得任意小.

如果 X 的维数最多的是 d, 就取最小的 d, 并且定义 X 的**拓扑维数**是 d. 于是又可以证明这个定义对于初等几何学里的熟悉的图形给出了 "正确的" 维数.

第四个直觉的思想会给出所谓的**同调与上同调维数**. 对于适当的拓扑空间, 都附有一个系列的群, 即*同调与上同调群*[IV.6 §4]. 在此只讨论同调群. 但是也可以很类似地讨论上同调群. 粗略地说, 第 n 个同调群说的是有多少本质不同的从闭 n 维流形 M 到 X 的连续映射. 如果 X 的维数小于 n, 可以证明第 n 个同调群是平凡的, 在一定意义下讲, 这就是说 X 中没有充分的空间来定义除常值映射以外的从闭 n 维流形 M 到 X 的有意义的映射. 另一方面, n 维球自身的第 n 个同调群就是 $\mathbf{Z}$, 就是说, 可以用一个整数参数来对从 n 维球到其自身的映射进行分类.

①原书下标错了. —— 中译本注

所以, 下面的说法是很有诱惑力的: 如果在一个空间里有足够的地方来容纳有意义的从 n 维流形到其内的映射, 则这个空间至少是 n 维的. 这个想法引导到了一大类维数的定义. 一个结构 X 如果有某个子结构有非平凡的第 n 个同调群, 则最大的 n 就定义为 X 的维数 (必须要考虑子结构, 因为如果有**过多的**空间, 同调群也可能是平凡的, 因为这时很容易把一个连续映射变形为一常值映射). 然而, 同调是一个很一般的概念, 而有许多不同的同调, 从而就有许多不同的同调维数的概念, 其中有一些是几何的概念, 但是代数结构也会有同调理论, 例如, 应用适当的理论就可以定义代数结构如环[III.81 §1] 或群[I.3 §2.1] 的同调群, 这是几何思想在代数上得到报偿的好例子.

现在转到关于维数的第五个也是最后一个 (至少是就本文而言) 直觉的思想, 即如何度量大小. 如果想讲述一个形体 X 的大小, 那么一个好方法是: 如果 X 是 1 维的, 就告诉他长度; 如果是 2 维的, 就告诉他面积; 3 维的就告诉他体积. 当然, 这里已经预先假设知道维数, 但是, 我们会看到, 有一个方法, 在没有事先判定维数以前, 就有办法知道哪一个度量最为适当. 这样就扭转了局面: 可以定义相应于最适当的度量的数就是维数.

为了做这件事, 我们要利用这样一个事实, 即当把形体放大时, 长度、面积和体积各按不同的尺度变化. 如果取一条曲线, 把它 (在各个方向上) 都按因子 2 放大, 则长度也会加倍. 更一般地说, 如果按因子 C 放大, 则长度会被乘以因子 C. 然而, 如果取一个 2 维形体, 并按因子 C 放大, 则面积会被乘以因子 C^2(粗略地说, 这个形体的每一个小部分都 "在两个方向上" 各放大了一个因子 C, 所以, 需要把面积用 C 乘两次). 3 维形体要乘以 C^3, 例如半径为 3 的球体的体积是半径为 1 的球体的体积的 27 倍.

这样的作法, 看起来似乎需要决定我们是先讨论长度、面积还是体积, 才能够开始考虑当形体放大时取哪一个尺度因子, 但是情况并不是这样的. 例如, 如果按因子 2 放大一个正方形, 就会得到一个新的正方形, 它可以分成四个与原来的正方形全等的小正方形. 所以, 用不着事前决定要讨论面积, 我们就能说新正方形的大小是原正方形的四倍.

看到了这一点会得出一个引人注目的推论: 有一些集合可以很自然地指定一个非整数的维数! 可能最简单的例子就是最先由康托[VI.54] 所发现而且现在就名为**康托集**的集合, 它是这样构造出来的: 从闭区间 $[0\,,\,1]$ 开始, 称它为 X_0. 然后把它的中间的三分之一除去, 即把 1/3 到 2/3 之间的数除去, [但是保留这两个数], 这样构成集合 X_1. 所以, X_1 是两个闭区间 $\left[0\,,\,\frac{1}{3}\right]$ 和 $\left[\frac{2}{3}\,,\,1\right]$ 之并. 下一步把这两个闭区间的中间三分之一除去, [但保留它们的端点, 所以除去的仍是开区间], 这样

得到 X_2, 所以 X_2 是四个闭区间 $\left[0,\dfrac{1}{9}\right]$, $\left[\dfrac{2}{9},\dfrac{1}{3}\right]$, $\left[\dfrac{2}{3},\dfrac{7}{9}\right]$ 以及 $\left[\dfrac{8}{9},1\right]$ 之并.

一般地说, X_n 是一些闭区间之并, 而 X_{n+1} 则是从这些闭区间除去中间的三分之一 [但保留端点] 所得的集合 —— 所以它是由一些闭区间所组成的, 这些闭区间的个数是组成 X_n 的闭区间的个数的两倍, 但是每一个组成的闭区间大小只是前一步所得的闭区间的三分之一. 得出了系列 $X_0, X_1, X_2, \cdots$ 以后, 它们的交就是康托集, 就是说, 不论把删除中间三分之一的步骤作了多少次, 始终会留下来的实数的集合就是康托集. 不难证明, 这些点就是其三进小数展开式中只有数码 0 和 2 那些数 (有些数有两个不同的三进小数式, 例如 1/3 既可以写成 0.1 也可以写成 $0.02222\cdots$[①]. 遇到这种情况宁可取循环的无限展开式, 而不用有限展开式. 总之, $\dfrac{1}{3}$ 属于康托集). 事实上, 当在第 n 步除去中间三分之一时, 就把三进小数 (而不是十进小数) 的小数点后第 n 位为 1 的那些数都删去了.

康托集有许多有趣的性质, 例如它是*不可数的*[III.11], 但是它的*测度*[III.55] 为 0. 其证明要点如下: 第一个论断来自这样的事实, 给出自然数集合的任意子集合 A, 就会得到康托集的一个不同的元 (只需取这样的三进数 $0.a_1a_2a_3\cdots$, 使得当 $i\in A$ 时, 令 $a_i=2$, 否则, 令 $a_i=0$), 而自然数集合有不可数多的子集合, 所以康托集是不可数的. 为了论证第二个论断, 注意 X_n 的小区间的总长度为 $\left(\dfrac{2}{3}\right)^n$(因为在构造 X_n 时, 我们把 X_{n-1} 的三分之一删去了). 因为康托集包含在每一个 X_n 内, 所以它的测度必定对于任意的 n 都小于 $\left(\dfrac{2}{3}\right)^n$, 这就意味着它的测度一定为零. 所以康托集从一个角度来看是很大的集合, 而从另一个角度来看又是很小的集合.

康托集的另一个进一步的性质是它的自相似性. 集合 X_1 由两个闭区间构成, 如果只看其中一个, 而不断地把中间三分之一除去, 所看见的就是整个康托集的构造过程, 只不过按因子 3 缩小了. 就是说, 康托集是由它自己的两个复本构成的, 而每一个复本都按因子 3 缩小. 由此得到以下的命题: 如果把康托集放大 3 倍, 就可以把这个放大的康托集分成全等的两个, 所以恰好是 "两倍大".

这件事对于康托集的维数有什么推论呢? 如果它的维数是 d, 则放大以后康托集的形体应该是 3^d 倍大. [但是现在只是 2 倍大], 所以 $3^d=2$, 而维数 d 应该是 $\log 2/\log 3$, 即约为 0.63 .

一旦知道了这一点, 康托集的神秘性就减少了. 我们马上就会看到, 可以建立一个分数维的理论, 而且具有一个有用的性质, 即可数多个维数至多为 d 的集合, 其并也最多只有维数 d. 所以, 康托集的维数大于零这一点就说明, 康托集不可能是可数集合 (因为单个点的维数为 0). 另一方面, 康托集的维数小于 1, 所以它比一个 1 维集合要小得多, 所以毫不奇怪, 它的测度为 0(这有一点像说曲面没有体积, [但

①原书有误. —— 中译本注

是曲面和 3 维物体的维数分别是 2 和 3, 而康托集与 1 维集合的维数分别是 0.63 和 1]).

分数维的理论中, 最有用的是豪斯道夫[VI.68] 发展起来的那一种. 我们先从一个称为豪斯道夫测度的概念开始, 这是一个很自然的评估一个 "d 维体积" 的办法, 甚至当 d 不是整数时也能用. 设有一条 $\mathbf{R}^3$ 中的曲线, 而想这样来做出其长度, 可以用球体覆盖这条曲线容易的程度来计算曲线的长度. 第一个想法是看怎样使得覆盖的球的直径之和为最小, 并以这个最小的长度为曲线的长度. 但是这是不行的, 可能走运遇到一条很长的曲线, 但是它缠得很紧, 以至于只需要一个直径很小的球体就把它覆盖起来了.

然而, 如果要求所用的球很小, 就不会发生这个情况了. 所以设所有的小球的直径最多为 δ. 令所有小球直径之和能够达到的最小值是 $L(\delta)$. δ 越小, 活动的余地也越小. 所以, 当 δ 趋于零时, $L(\delta)$ 趋于一个极限 L(可能是无穷大), 就称 L 为曲线的长度.

现在设有一个 $\mathbf{R}^3$ 中的光滑曲面, 我们要看一看从用小球去覆盖曲面中能够得到什么信息. 这一次, 用很小的球 (小到只与曲面的一部分相交, 而这一部分几乎是平坦的) 能够覆盖的曲面面积大体上是与球的直径的**平方**成正比. 只有这一点是需要变动的细节: 如果覆盖整个曲面的小球的直径最多为 δ, 令 $A(\delta)$ 为所有这些小球的直径的平方和所能达到的最小值, 我们就宣布曲面的面积是当 $\delta \to 0$ 时 $A(\delta)$ 的极限 (严格地说, 还应该用 $\pi/4$ 去乘这个极限, 但是那样一来, 我们得到的面积定义就不那么容易推广了).

我们刚才得到了定义 $\mathbf{R}^3$ 中的形体的长度和面积的一个方法. 这两种度量的仅有的差别在于: 对于长度, 我们考虑小球的直径之和, 而对于面积, 则考虑直径的**平方和**. 一般地, 可以用类似的方法定义 **d 维的豪斯道夫测度**, 只要应用直径的 d 次方的和就行了.

我们可以用豪斯道夫测度的概念来严格地定义分数维. 不难证明, 对于任意的形体 X, 都能找到一个在以下意义下的合适的 d: 如果取 $c < d$, 则 X 的 c 维豪斯道夫测度为 0, 而如果 $c > d$, 则 c 维豪斯道夫测度为无穷大 (例如对于光滑曲面的 c 维豪斯道夫测度, 当 $c < 2$ 时应为 0, 而当 $c > 2$ 时为无穷大). 这样得到的 d 就称为形体 X 的豪斯道夫维数. 它在分析分形集合时是很有用的, 这一点详见动力学[IV.14].

重要的是要认识到, 一个集合的豪斯道夫维数不一定等于它的拓扑维数. 例如康托集, 其拓扑维数是 0, 但是豪斯道夫维数是 $\log 2/\log 3$. 一个更大的例子是 Koch 雪花, 它是一个非常细的锯齿形的曲线. 因为它是一条曲线 (从而一个点就可以把它切成两段), 所以它的拓扑维数是 1. 然而因为它的非常细的锯齿形, 它的长度是无穷大, 所以可以证明它的豪斯道夫维数是 $\log 4/\log 3$.

III.18 广义函数
(Distributions)

陶哲轩 (Terence Tao)

一个函数正常地是定义为这样一个对象 $f: X \to Y$, 它对集合 X 的任意点 x 都指定另一个集合 Y 中一点 $f(x)$, X 通常称为这个函数的**定义域**, 而 Y 称为其**值域**(见数学的语言和语法[I.2 §2.2]) 这样, 函数的定义是集合论的, 而其基本的运算是**赋值**, 即给定了 X 的元素 x, 可以求出 f 在 x 处的值, 即 Y 中的 $f(x)$.

但是在许多数学领域里, 这并不是描述函数的最好方法. 例如在几何学里面, 一个函数的基本性质并不一定是它如何作用在点上, 而是它如何把比点更复杂的对象 (如其他函数, 丛 [IV.6 §5] 和截口、概型[IV.5 §3] 和束等等)**推前或拉回**. 类似于此, 在分析中, 函数也不一定要就它如何作用于点来定义, 而是就它如何作用于不同种类的对象如集合或其他函数来定义; 前者导致**测度**的概念, 而后者导致**广义函数**(或称**分布**) 的概念.

当然, 所有这些关于函数或类似函数的对象的概念都是互相关联的. 在分析中, 认为函数的各种概念构成了一个很广的谱是有益处的, 非常 "光滑的" 函数列在谱的一端, 而非常 "粗糙的" 函数则位于谱的另一端. 光滑的函数类对于 "成员" 资格是很有限制的, 这意味着它们有好的性质, 可以对它们进行多种运算 (例如微分), 但是这也意味着不能保证我们正在处理的恰好就是属于这个范畴的函数. 与此相反, 粗糙的函数类是很一般的包括甚广的, 很容易确定, 我们正在处理着它们, 但是要付出的代价是能够对它们进行的运算时常会急剧减少 (见函数空间[III. 29].

虽然如此, 不同的函数类时常可以用统一的方法来处理, 因为粗糙的函数时常可以用光滑的函数 (在适当的拓扑[III. 90] 下) 任意好地逼近. 然后, 给出一个对于光滑的函数有自然定义的运算时, 很有机会恰好有一种自然的方法把它推广为对于粗糙的函数的运算, 就是对于粗糙的函数找到用光滑的函数越来越好地逼近它们的序列, 再对光滑的函数施行这个运算, 并且取极限.

广义函数(或称**分布**) 就位于这个谱的粗糙的一端, 但是在我们指出广义函数究竟是什么以前, 先提一下更光滑的函数是有帮助的, 这部分地是为了作比较, 部分地是因为我们将要用所谓**对偶性**的过程来从光滑的函数类得出粗糙的函数类, 其方法如下: 定义在函数空间 E 上的**线性泛函**只不过就是由 E 到标量 $\mathbf{R}$ 或 $\mathbf{C}$ 的线性映射. 在典型情况下, E 是一个赋范空间, 至少是具有一种拓扑, 而其上的连续线性泛函的空间就称为**对偶空间**.

解析函数类 $C^{\omega}[-1,1]$. 在许多方面它是所有函数中"最好"的, 其中包括了许多我们熟悉的函数例如 $\exp(x)$, $\sin x$ 还有多项式等等. 然而, 我们不去进一步讨论它们, 因为对于许多目的, 这个函数类因过于严格而不好用 (例如, 一个解析函数值只要在一个区间上为零, 就会处处为零).

试验函数类 $C_c^{\infty}[-1, 1]$. 它们是定义在区间 $[-1, 1]$ 上的光滑函数 (即无穷可微) 的且在 $-1, 1$ 两点附近恒为零的函数 f 的空间 (所谓"在 -1 , 1 两点附近恒为零", 就是说, 能够找到一个常数 δ , $0<\delta<1$, 使得在 $x>1-\delta$ 或 $x<-1+\delta$ 时, $f(x)=0$①), 它们比解析函数更容易处理②. 例如可以用它们来构造出光滑的"截断函数", 就是在一个小的集合之外恒为 0, 而在其内不恒为 0 的函数. 还有微积分中的所有运算 (微分、积分、复合、卷积、赋值等等) 对它们都可以施行.

连续函数类 $C^0[-1, 1]$. 这些函数对于赋值运算 $x \mapsto f(x)$ 是足够正规的, 所以对于每一点 $x \in [-1, 1]$, $f(x)$ 都有意义, 对于这些函数可以进行积分和例如乘法或者复合这样的代数运算, 但是对于在其上进行微分运算就不够正规了. 然而, 它们仍然被认为是分析中比较光滑的函数的例子.

平方可积函数类 $L^2[-1, 1]$. 这些函数 $f:[-1, 1] \to \mathbf{R}$ 就是在区间 $[-1, 1]$ 上可测而且其勒贝格积分 $\int_{-1}^{1}|f(x)|^2\,\mathrm{d}x$ 为有限的函数类. 如果有两个这样的函数 f 和 g, 使得 $f(x) \neq g(x)$ 的 x 之集合为零测度集合, 通常就认为这两个函数是相同的 (所以, 从集合论的观点看来, 所讨论的对象其实是一个等价类 [I.2 §2.3]. 因为单元素集合 $\{x\}$ 是零测度集合, 所以, 可以改变一个函数在一点之值 $f(x)$ 而不改变这个函数. 这样, 对于平方可积函数 $f(x)$, 在一个特定点 x 赋值是没有意义的. 然而两个只在一个零测度集合上相异的函数具有相同的勒贝格积分[III.55], 所以积分仍然是有意义的.

关于这个函数类关键一点在于它在以下意义下是自对偶的: 这个函数类中的任意两个函数都可以用**内积** $\langle f, g\rangle=\int_{-1}^{1} f(x)\,g(x)\,\mathrm{d}x$ 来配对. 因此, 给定一个函数 $g \in L^2[-1, 1]$, 映射 $f \mapsto \langle f, g\rangle$ 定义一个 $L^2[-1, 1]$ 上的线性泛函, 而且它是连续的. 进一步, 给定任何一个 $L^2[-1, 1]$ 上的连续线性泛函 ϕ, 必存在唯一的函数 $g \in L^2[-1, 1]$, 使得对任意的 $f \in L^2[-1, 1]$, 都有 $\phi(f)=\langle f, g\rangle$. 这是里斯 (Frigyes Riesz, 1880–1956, 匈牙利数学家)**表现定理**之一的一个特例.

有限波莱尔测度类 $C^0[-1, 1]^*$. 任意的有限波莱尔测度[III.55] μ 都给出 $C^0[-1, 1]$ 上的一个连续线性泛函如下: $f \mapsto \langle\mu, f\rangle=\int_{-1}^{1} f(x)\,\mathrm{d}\mu$. 另一个里斯表现定理指出, $C^0[-1, 1]$ 上的所有连续线性泛函都是这样产生的, 所以, 在

①原书有小的错误 —— 中译本注

②原书说它们比解析函数更多, 这一点不恰当, 因为解析函数不可能在这一函数类中.—— 中译本注

原则上, 可以定义有限波莱尔测度即为 $C^0[-1,1]$ 上的连续线性泛函.

分布①类 $C_c^\infty[-1,1]^*$. 正如有限波莱尔测度可以看成是 $C^0[-1,1]$ 上的连续线性泛函一样, 一个分布 μ 就是 $C_c^\infty[-1,1]$(带有适当的拓扑) 上的连续线性泛函. 这样, 分布就可以看作是一个 "虚拟的" 函数: 它自己不能直接赋值, 甚至不能在一个开集合上积分, 但是它仍然可以和一个试验函数 $g \in C_c^\infty[-1,1]$ 配对, 生成一个数 $\langle\mu, g\rangle$. 一个著名的例子是狄拉克分布 δ_0, 其定义是一个泛函, 在与任意试验函数 g 配对后都生成 g 在 0 点的值 $g(0)$: $\langle\delta_0, g\rangle = g(0)$. 类似地, 也有狄拉克分布的导数 $-\delta_0'$, 它与任意试验函数 g 配对后则生成 g 在 0 点的导数值 $g'(0)$: $\langle-\delta_0', g\rangle = g'(0)$ (加一个负号的理由将在后面解释). 因为试验函数上允许那么多的运算, 所以有许多方法在其上定义连续的线性泛函, 于是, 分布类是很大的. 尽管如此, 尽管分布的非直接的虚拟的本性, 仍然可以在其上定义许多运算, 这一点下面再讨论.

超函数类 $C^\omega[-1,1]^*$. 还有一些函数类比分布类更大, 例如超函数, 粗略地想, 它只能作用于解析函数 $g \in C^\omega[-1,1]$, 而不能作用于试验函数 $g \in C_c^\infty[-1,1]$. 然而, 因为解析函数类太稀疏了, 超函数在分析中就不如分布类那么有用.

初看起来, 广义函数的概念只有有限的用途, 因为所有的广义函数 μ 只被作用于试验函数 g 以生成内积 $\langle\mu, g\rangle$. 然而利用这样的内积, 就可以利用对偶性, 把原来只定义在试验函数上的运算, 扩展到广义函数上去. 微分是一个典型例子. 设想要求一个广义函数 μ 的导数 μ', 也就是想要问如何对任意试验函数 g 和广义函数 μ 定义 $\langle\mu', g\rangle$. 先考虑 μ 本身也是一个试验函数 f 的情况, 这时, 可以利用分部积分方法来计算 $\langle\mu', g\rangle$ 如下 (记住试验函数在 -1 和 1 两点为零):

$$\langle f', g\rangle = \int_{-1}^{1} f'(x)\, g(x)\, \mathrm{d}x = -\int_{-1}^{1} f(x)\, g'(x)\, \mathrm{d}x = -\langle f, g'\rangle .$$

注意, 因为 g 是一个试验函数, 所以 g' 也是. 所以, 可以对任意的广义函数 f 定义其导数: $\langle\mu', g\rangle = -\langle\mu, g'\rangle$. 这也就说明了狄拉克分布的导数公式里面出现负号的正当性: $\langle\delta_0', g\rangle = -\langle\delta_0, g'\rangle = -g'(0)$.

---

① 推广函数概念使之包括例如 δ 函数这些 "奇异" 的对象, 早在 19 世纪末到 20 世纪初就有这样的企图了. 到 20 世纪 40 年代, 法国数学家施瓦兹 (Laurent-Moïse Schwartz, 1915–2002) 非常系统地处理了这个问题, 并于 1950–1951 年出版了《分布理论》(*Thérie des Distributions*) 两卷, 提出了系统的理论. 他指出有限波莱尔测度就是函数概念的一个推广. 由于这个测度的物理原型就是质量的分布, 所以他把自己的理论名为分布理论. 到 20 世纪 50 年代, 前苏联数学家盖尔范德 (Israel Moiseevich Gelfand, 1913–2009) 和他的学生们发表了《广义函数论》五卷, 极大地扩大了其应用领域, 加深了其理论基础. 因此后来许多人愿意使用广义函数这个名称. 我国引入这个理论主要是受到盖尔范德学派的影响, 所以我国文献中, 更多地使用广义函数一词. 本文中, 我们就常用广义函数一词来代替分布一词 (又, 原书把记号 $C_c^\infty[-1,1]^*$ 误为 $C^\infty[-1,1]^*$). —— 中译本注

比较形式的说法是我们在此所做的情况无非是计算了微分算子 $\frac{\mathrm{d}}{\mathrm{d}x}$ 的伴算子. 这个算子本来只定义在稠密的试验函数空间里, 现在再取其伴, 作为一般的广义函数的导数的定义. 这个过程是适当定义的, 而且对于许多其他运算也是适用的, 例如, 可以把两个广义函数加起来, 也可以用一个光滑函数去乘广义函数, 作两个广义函数的卷积, 从左方或右方把广义函数与适当的光滑函数复合起来, 甚至可以作广义函数的傅里叶变换. 例如狄拉克分布的傅里叶变换就是常值函数 1, 反过来也对 (这在本质上就是傅里叶变换的反演公式), 而 $\sum_{n\in\mathbf{Z}}\delta_0(x-n)$ 是它自己的傅里叶变换 (这在本质上就是泊松 (Siméon-Denis Poisson, 1781 –1840, 法国数学家) 求和公式. 所以广义函数是一个在其中很好工作的空间, 因为它包含了很大的函数类 (例如所有的测度、可积函数), 同时它在分析中的许多通常的运算下都是封闭的. 因为试验函数在广义函数空间里是稠密的, 定义在广义函数上的运算通常也都与定义在试验函数上的同一运算是相容的. 例如, 设 f 和 g 都是试验函数, 而且在广义函数意义下有 $f'=g$, 则此式在经典意义下也成立. 这时常使我们在处理广义函数时, 可以把它们当作试验函数一样, 而不必担心会发生混淆或有不准确的地方. 唯一需要小心处理的主要运算是广义函数的赋值与逐点的乘法, 二者通常对于广义函数都没有适当的定义 (例如狄拉克的 δ 函数的平方作为广义函数就没有适当的定义).

另一种看待广义函数的观点是视它为试验函数的**弱极限**. 我们说函数序列 f_n **弱收敛**于一个广义函数 μ, 就是说对于任意的试验函数 g 都有 $\langle f_n, g\rangle\to\langle\mu, g\rangle$. 举一个例子, 如果 φ 是一个试验函数, 而且积分为 1, $\int_{-1}^{1}\varphi(x)\,\mathrm{d}x=1$, 则可以证明 $f_n(x)=n\varphi(nx)$ 弱收敛于狄拉克 δ 分布 δ_0; $f_n'(x)=n^2\varphi'(nx)$ 弱收敛于 δ_0'. 另一方面, $g_n(x)=\cos nx\varphi(x)$ 弱收敛于 0(这是**黎曼–勒贝格引理**的一个变体). 这样, 弱收敛有一些在较强的收敛概念下不会出现的不平常的特性, 就是强烈的振荡有时会"消失". 用广义函数而不用更光滑的函数还有一个好处, 就是广义函数空间在弱收敛下, 时常会有某种紧性 [例如有巴拿赫–Alaoglu (Leonidas Alaoglu, 1914–1981, 加拿大的希腊裔数学家) 定理]. 所以广义函数可以看成是更加光滑的函数的性态的渐近的极限, 正如实数可以看成是有理数的极限一样.

因为广义函数可以容易地微分, 而仍与更光滑的函数有密切的联系, 所以它对于研究偏微分方程 (以下简称 PDE) 极为有用, 特别是研究线性的 PDE. 例如线性 PDE 的一般的解时常是用它的**基本解**来表示的, 而基本解则是在广义函数意义下解出这个 PDE 的. 更一般地说, 广义函数理论 (加上一些相关的概念, 例如**弱导数**) 后, 会给出一种 (当然不是唯一的一种) 定义线性和非线性 PDE 的**广义解**的方法. 所谓广义解, 顾名思义, 推广了光滑解 (亦称**经典解**) 的定义, 广义解允许解有奇异性形成、激波和其他非光滑的性态. 在有些情况下, 构造 PDE 的光滑解最容易的

方法是首先构造出广义解，再用附加的论证来证明广义解其实是光滑的.

III.19 对　偶　性
(Duality)

对偶性是一个在数学的各个领域几乎都会出现的重要主题. 一再地出现这样的情况：可以对一个数学对象附加上一个相关的"对偶的"对象，这能够帮助我们理解原来对象的性质. 尽管对偶性在数学中如此重要，却没有一个单独的定义能够覆盖这个现象的各个例子. 所以，我们只来看一些例子以及它们所展示的一些特性.

1. 柏拉图的正多面体

设取一个正立方体，在它的六个面上画出其中心，并以它们为顶点作一个新的正多面体，这样得到的多面体将是一个正八面体. 如果继续这个做法会得到什么？在这个八面体的八个面上各画出其中心，就会发现，它们将是一个正立方体 (即正六面体) 的八个顶点. 我们说，正立方体和正八面体互相**对偶**. 对于其他的柏拉图正多面体也可以这样做，于是可以看到正十二面体和正二十面体互相对偶，而正四面体的对偶仍是正四面体.

上面描述的对偶性不只是把五个柏拉图正多面体进行了分类，它使我们能把关于一个正多面体的命题与关于其对偶的命题联系起来. 例如，一个正十二面体的两个面如果共有一棱，这两个面就是相邻的，而它们共有一棱当且仅当其对偶的二十面体的相应顶点有一条棱相连接. 由此原因，在十二面体的棱与二十面体的棱之间也就建立了对应关系.

2. 射影平面上的点与直线

射影平面[I.3 §6.7]有几个等价的定义，其中之一，也就是在这里将要使用的：射影平面就是 $\mathbf{R}^3$ 中过原点的直线的集合. 这些直线就成为射影平面上的"点". 为了使这个"点"更像一个点，就把这个"点"，即过原点的直线，与 $\mathbf{R}^3$ 中的一对点，即此直线与 [球心在原点] 的单位球面的交点，对应起来，说实在的，射影平面可以定义为将对径点 (即一条直径的两端的点) 视为同一点单位球面.

射影平面上的典型的"直线"就是位于过原点的某一平面上的"点"(即过原点的直线) 的集合，它对应于这个平面截球面所成的大圆，当然大圆上的对径点要视为同一点.

射影平面上的点与直线有一个自然的联系：每一个点 P 都与 [$\mathbf{R}^3$ 中] 正交于 P 的点所成的直线 L 相联系，而每一条直线 L 也都与单一的一个点相联系，这个点正交于直线上所有的点. 例如，设 P 为 z 轴，则与它相联系的射影直线 L 就是

所有过原点而且位于 xy 平面上的直线的集合, 反过来也对. 这样的联系有以下的基本性质: 如果点 P 属于直线 L, 则与 P 相联系的直线, 必包括与 L 相联系的点.

这就允许我们把关于点和直线的定理翻译为逻辑上等价的关于直线和点的定理. 例如, 三个点共线 (即位于同一直线上) 当且仅当与它们相联系的直线共点 (即经过同一点). 一般说来, 如果在射影几何中得到了一个定理, 就可以不花一点力气得到另一个对偶的定理 (除非对偶定理和原定理是完全一样的).

3. 集合和余集合

令 X 为一个集合, A 为 X 的任意子集合, 则 A 的余集合 A^c 就是由 X 中的不属于 A 的元素组成的集合. A 的余集合的余集合显然就是 A 自己, 所以, 在集合和余集合之间就有一种对偶性. 德 • 摩根定律指出, 如果 A 和 B 都是 X 的子集合, 则 $(A\cap B)^c = A^c \cup B^c$, $(A\cup B)^c = A^c \cap B^c$. 这种互余性质 “把交变为并”, 反过来也对. 注意, 如果对 A^c 和 B^c 应用德 • 摩根的第一个定律, 就有 $(A^c \cap B^c)^c = A \cup B$, 再对双方求其余集合, 立刻得到第二定律.

因为有了德 • 摩根定律, 任意涉及并和交的等式, 在交换并和交以后仍然成立. 例如有一个有用的恒等式 $A\cup(B\cap C) = (A\cup B)\cap(A\cup C)$. 应用此式于余集合, 再用德 • 摩根定律, 就会直接得到一个同样有用的恒等式

$$A\cap(B\cup C) = (A\cap B)\cup(A\cap C).$$

4. 对偶向量空间

令 V 为例如 $\mathbf{R}$ 上的向量空间[I.3 §2.3]. 其**对偶空间** V^* 就定义为 V 上的**线性泛函**的空间, 就是说, 由 V 到 $\mathbf{R}$ 的所有线性映射的集合. 不难定义线性泛函之间的加法和以标量乘线性泛函的运算, 使得 V^* 也成为一个向量空间.

设 T 为由向量空间 V 到另一个向量空间 W 的线性映射[I.3 §4.2]. 如果给了对偶空间 W^* 中的一个元素 w^*, 就可以用 T 和 w^* 来生成 V^* 中的元素 v^*: 作一个把 v 映为实数 $w^*(Tv)$ 的映射, [并记它 $(T^*w^*)(v)$]. 这里面包含了两个映射, 其一是把 v 映为 $w^*(Tv)$. 很容易验证这第一个映射对于 v 是线性的, 因此 T^*w^* 是 V^* 的元素, [记它为 v^*, 这样就产生了由 W^* 到 V^* 的第二个映射: $T^*: W^* \to V^*$, 它把 w^* 映到 V^* 中的 $T^*w^* = v^*$. 很容易验证第二个映射 T^*w^* 对于 w^* 是线性的, 这样 T^*w^* 就是由 W^* 到 V^* 的线性映射]. 这个映射称为 T 的**伴映射**.

这是对偶性的典型特性: 一个由对象 A 到对象 B 的函数, 非常常见地导出一个由 B 的对偶到 A 的对偶的函数.

设 T^* 是一个满射. 如果 $v \neq v'$, 必可找到一个 v^* 使 $v^*(v) \neq v^*(v')$, 然后由于 T^* 是一个满射, 所以必有 W^* 中的元素 w^*, 使得 $T^*w^* = v^*$, 所以 $T^*w^*(v) \neq T^*w^*(v')$. 这意味着 $w^*(Tv) \neq w^*(Tv')$, 亦即 $Tv \neq Tv'$, 而 T 是一个单射. 也可以

证明, 如果 T^* 是一个单射, 则 T 是一个满射. 事实上, 如果 T 不是满射, 则 TV 是 W 的真子空间, 这使我们能够找到 W 的一个线性泛函 w^*, 使得对于每一个 $v \in V$ 均有 $w^*(Tv) = 0$, 从而 $T^*w^* = 0$, 这与 T^* 的单射性相矛盾. 如果 V 和 W 都是有限维空间, 则 $(T^*)^* = T$. 这时, 我们发现 T 为单射当且仅当 T^* 为满射, 反过来也对. 所以可以利用对偶性把存在问题转化为唯一性问题, [或者把唯一性问题转化为存在问题]. 这样把一类问题转化为另一类问题, 又是对偶性的一个很有用的特性.

如果一个向量空间还有附加的结构, 对偶空间的概念会有变化. 例如, 如果 X 是一个实巴拿赫空间[III.62], 则 X^* 定义为由 X 到 $\mathbf{R}$ 的**连续**线性泛函的空间, 而不是**所有**线性泛函的空间. 这个空间也是一个巴拿赫空间: 一个连续线性泛函 f 的范数定义为 $\sup\{|f(x)| : x \in X\ ,\ \|x\| \leqslant 1\}$. 如果对一个特定的巴拿赫空间 (例如在条目函数空间[III.29] 中所讨论的空间之一), 对偶空间有一个显式的表示, 这将是极为有用的. 这就是说, 我们很愿意找出一个显式描述的巴拿赫空间 Y 和一种把 Y 的非零元 y 和 X 上的一个非零的连续线性泛函 ϕ_y 联系起来的方法, 使得 X 的每一个连续线性泛函都等于相应于某个 $y \in Y$ 的 ϕ_y.

从这个角度看来, 把 X 和 Y 看成具有相同的地位是很自然的. 这一点反映在采用记号 $\langle x\ ,\ y\rangle$ 来代替记号 $\phi_y(x)$ 上. 如果我们这样做了, 就会把我们的注意力吸引到这样一件事实: $\langle\cdot\ ,\ \cdot\rangle$ 是一个把一个元素对 $(x\ ,\ y)$ 映为实数 $\langle x\ ,\ y\rangle$ 的映射, 这是一个从 $X \times Y$ 到 $\mathbf{R}$ 的连续的双线性映射.

更一般地说, 只要有两个数学对象的集合 A 和 B、某种 "标量" 的集合 S 以及一个对各个变元分别保持其结构的函数 $\beta:\ A \times B \mapsto S$, 都可以把 A 的元素看成 B 的对偶的元素. 像 β 这样的函数称为一个**配对**.

5. 极体 (极集合)

令 X 为 $\mathbf{R}^n$ 的一个子集合, 而 $\langle\cdot\ ,\ \cdot\rangle$ 是 $\mathbf{R}^n$ 上的标准内积[III.37]. 所谓 X 的**极集合**(polar, polar set)X^{c} 就是满足以下条件的 $y \in \mathbf{R}^n$ 的集合: 对于所有的 $x \in X$, $\langle x\ ,\ y\rangle \leqslant 1$. 不难证明 X^{c} 是一个闭凸集合, 而如果 X 本身就是一个闭凸集合, 则 $(X^{\mathrm{c}})^{\mathrm{c}} = X$. 此外, 若 $n = 3$ 而 X 是一个以原点为中心的柏拉图正多面体, 则 X^{c} 是对偶的柏拉图正多面体 (的倍数), 而若 X 是一个赋范空间的 "单位球体"(即范数不大于 1 的点的集合), X^{c} 也容易验证可以等同于对偶空间的单位球体.

6. 阿贝尔群的对偶

若 G 是一个阿贝尔群, 则 G 上的一个**特征标**定义为由 G 到模为 1 的复数之群 $\mathbf{T}$ 的同态. 两个特征标可以以显然的方式相乘, 这种乘法使得 G 的所有特征标也成为一个群, 称为 G 的**对偶群**, 记作 $\hat{G}$. 此外, 如果 G 具有某种拓扑结构, 则这里的同态还要求为连续同态.

群 G 就是 $\mathbf{T}$ 的情况是一个重要的例子. 不难证明, 由 $\mathbf{T}$ 到 $\mathbf{T}$ 的连续同态一定具有以下的形式: $\mathrm{e}^{\mathrm{i}\theta} \mapsto \mathrm{e}^{\mathrm{i}n\theta}$, 其中 n 是一个整数 (可以是负整数或 0). 这样, $\mathbf{T}$ 的对偶群就是 (即同构于)$\mathbf{Z}$.

群之间的这种形状的对偶称为**庞特里亚金**(Lev Semenovich Pontryagin, 1908 – 1988, 前苏联数学家) **对偶性**. 注意, 现在很容易定义 G 与 $\hat{G}$ 之间的配对: 给定了 G 的一个元素 $g \in G$ 与 $\hat{G}$ 的一个元素 $\psi \in \hat{G}$, [因为 $\hat{G}$ 的元素就是由 G 到 $\mathbf{T} = \{z, |z| = 1\}$ 的同态, 所以 $\psi(g) \in \mathbf{T} \subset \mathbf{C}$ 是一个标量], 我们就用这个标量来定义 "内积" $\psi(g) = \langle g, \psi \rangle$.

在适当的条件下, 这个配对可以拓展为定义在 G 和 $\hat{G}$ 上的函数. 例如, 当 G 和 $\hat{G}$ 都是有限群的时候, 若 $f: G \to \mathbf{C}$, $F: \hat{G} \to \mathbf{C}$, 则可以定义 $\langle f, F \rangle = |G|^{-1} \sum\limits_{g \in G} f(g) F(\psi)$, 这是一个复数. 一般情况下, 可以得到 G 上的函数的*复希尔伯特空间*{III.37}与 $\hat{G}$ 上的函数的复希尔伯特空间之间的配对.

这个扩展的配对又导致另一个重要的对偶性. 给定了希尔伯特空间 $L^2(\mathbf{T})$ 里的一个函数 $f \in L^2(\mathbf{T})$, 它的**傅里叶变换**是一个函数 $\hat{f} \in l^2(\mathbf{Z})$, 其定义是

$$\hat{f}(n) = \frac{1}{2\pi} \int_0^{2\pi} f\left(\mathrm{e}^{\mathrm{i}\theta}\right) \mathrm{e}^{-\mathrm{i}n\theta} \mathrm{d}\theta.$$

傅里叶变换也可以对于其他的阿贝尔群上的函数类似地定义, 在许多数学领域里具有极大的重要性 (例如可见条目*傅里叶变换*[III.27] 和*表示理论*[IV.9]). 和前面几个例子比较起来, 把关于一个函数的命题翻译成为关于其傅里叶变换的等价的命题并不总是很容易的, 但是, 傅里叶变换的力量也就在此: 如果想要理解定义在 $\mathbf{T}$ 上的函数 f, 就可以同时来探讨 f 和 $\hat{f}$ 二者的性质. 有些性质可以从表现为关于 f 的事实中很自然地得出, 而另一些性质则可以从表现为关于 $\hat{f}$ 的事实中很自然地得出. 所以, 傅里叶变换把 "人的数学的力量翻了一番".

7. 同调与上同调

令 X 为一个紧 n 维*流形*[I.3 §6.9]. 若 M 和 M' 分别是其 i 维和 $n-i$ 维子流形, 而它们又都有较好的形态, 并处于充分一般的位置, [即其性态与相交情况均无太奇特和退化之处, 具体的条件有待进一步明确], 则它们将会相交于一个有限点集合上. 若对每一个交点都自然地附上 $+1$ 或 -1 来表示它们相交的具体情况, 则在这些点处的这些数之和将是一个不变量, 称为 M 和 M' 的相交数. 这个数可以证明只依赖于 M 和 M' 的*同调类*[IV.6 §4]. 这样, 相交数就定义了一个由 $H_i(X) \times H_{n-i}(X)$ 到 $\mathbf{Z}$ 的映射, 这里 $H_r(X)$ 是 X 的第 r 个同调群. 这个映射对每一个变元都分别是群同态, 所以产生一个配对而引导到所谓**庞加莱对偶性**, 最后又引导到现代的**上同调理论**, 而这是同调的对偶. 和前面的一些例子一样, 许多与

同调相关的概念, 对于上同调都有对偶的概念. 举一个例子, 在同调理论中有**边缘映射**, 而在上同调理论中则有**上边缘映射**(映射的方向与边缘映射相反). 另一个例子是一个由 X 到 Y 的连续映射生成由同调群 $H_i(X)$ 到同调群 $H_i(Y)$ 的同态, 也生成一个由上同调群 $H^i(Y)$ 到上同调群 $H^i(X)$ 的映射.

8. 本书中讨论到的其他例子

上面的例子远非完备, 甚至在本书也还有更多的例子. 例如在关于微分形式的条目 [III.16] 中就讨论了 k 形式和 k 维曲面的配对, 亦即对偶 (这个配对由在曲面上对此形式积分来给出). 关于分布的条目 [III.18] 讲述了如何利用对偶性来给类似于函数的对象, 例如狄拉克 δ 分布下严格的定义. 条目*镜面对称*[IV.16] 讨论了一个惊人的 (然而很大程度上仍然只是猜测的) 在Calabi-Yau *流形* [III.6] 与所谓 "镜面流形" 之间的对偶性. 镜面流形时常比原来的流形更容易理解, 所以这种对偶性也像傅里叶变换一样, 使得原来不可想象的计算成为可能. 条目*表示理论*[IV.9] 讨论了某些 (非阿贝尔) 群的 "朗兰茨对偶", 对这个对偶的适当的理解将会解决许多尚未解决的重大问题.

III.20 动力系统和混沌

(Dynamical Systems and Chaos)

从科学的观点看来, 一个动力系统就是一个随时间变化的物理系统, 如行星系或渠道里的水流. 典型情况是, 这个系统的各个部分在时刻 t 的位置和速度只依赖于恰好这个时刻以前各个部分的位置与速度, 这意味着这个系统的行为是由一组*偏微分方程*[I.3 §5.3] 来控制的. 一组非常简单的偏微分方程时常会导致物理系统的非常复杂的行为.

从数学观点看来, 一个动力系统则是按照精确的法则随时间演化的数学对象, 这个法则从这个系统恰好在时刻 t 以前的行为决定了它在时刻 t 的行为. 这里说的 "恰好在时刻 t 以前" 有时是讲的在无穷小时间段以前, 所以就涉及了微积分. 但是还有一个充满活力的**离散**动力系统理论, 在其中时间只取离散值, 而 "恰好在时刻 t 以前" 就是指的 $t-1$. 如果一个函数 f 告诉我们这个系统在时刻 t 是如何依赖于它在时刻 $t-1$ 的情况的, 这个系统从整体上看就是 f 的**迭代**, 即反反复复地用 f 作用于这个系统.

和连续的动力系统一样, 非常简单的函数 f, 如果迭代了充分多次, 会导致非常复杂的行为. 特别是有些最有趣的动力系统, 其中既有离散的, 也有连续的, 会展现出一种对于初始条件的极端的敏感性, 这就叫做**混沌**. 例如控制天气的方程式就是这样的. 我们不能期望精确地确定地球表面的每一个点处的风速 (更不说是在高

处的风速了), 就是说只能是有了近似的风速就过得去了. 因为相关的方程式是混沌的, 所得出的不准确的误差, 哪怕开始很小, 迅速地就传播开来, 马上就征服了整个系统, 可以从另一个同样很好的近似开始, 就会发现, 只要经过了很短的时间, 系统就会以一种完全不同的方式演化. 这就是为什么时间超出几天以后的准确预报是不可能的.

关于动力系统和混沌详见*动力学*[IV.14].

III.21 椭圆曲线
(Elliptic Curves)

Jordan S. Ellenberg

域 K 上的椭圆曲线可以定义为一条域 K 上的亏格为 1 的代数曲线, 其上的点的坐标在 K 中. 如果觉得这个定义太抽象, 还有一个等价的定义如下: 椭圆曲线就是下面的方程所决定的平面曲线:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \ . \tag{1}$$

只要 K 的特征不是 2, 就可以把它化为较简单的形式 $y^2 = f(x)$, 其中 f 是一个三次多项式. 在这个意义下, 椭圆曲线是一个很具体的对象. 然而, 这个定义已经催生了似乎有着无穷无尽的有趣的数学分支, 它是数论和代数几何的巨大的思想、例子和问题的宝藏. 这部分地是因为有许许多多的 "X" 的值都使得 "X 中的最简单而有趣的例子就是椭圆曲线".

例如, 坐标在 K 中的椭圆曲线 E 自然地构成一个阿贝尔群, 称此群为 $E(K)$. 一个连通的*射影簇*[III.95] 如果容许这样的阿贝尔群就称为一个**阿贝尔簇**, [记这个簇为 A, 而这里说的阿贝尔群则记为 $A(K)$]; 椭圆曲线就是一个 1 维的阿贝尔簇. 莫德尔 (Louis Joel Mordell, 1888 –1972, 英国数学家)–韦伊 (André Weil, 1906–1998, 法国数学家) 定理指出, 若 A 是阿贝尔簇, 而 K 是一个数域, 则 $A(K)$ 其实是一个**有限生成**的阿贝尔群, 称为**莫德尔–韦伊群**. 这些阿贝尔群虽然已经经过了大量的研究, 却仍然保留了许多神秘的地方 (见条目*曲线上的有理点与莫德尔猜想*[V.29]), 甚至当 A 是一条椭圆曲线时, 也还有许多我们并不知道的事情, 虽然 Birch-Swinnerton-Dyer *猜想*[V.4] 对于 $E(K)$ 的秩提出了一个猜想的公式. 关于椭圆曲线上有理点的更多知识可见*算术几何*[IV.5].

因为 $E(K)$ 是一个阿贝尔群, 则给定了素数 p 以后, 就可以研究适合条件 $pP = 0$ 的元素 P 所成的子群 $E(K)[p]$. 特别可以取域 K 的代数闭域 (algebric closure, 即一个域的代数闭的代数扩张)$\tilde{K}$ 并考虑 $E\left(\tilde{K}\right)[p]$. 于是, 如果 K 是一个

数域[III.63](或者就现在这个问题而言, 如果这个域不是特征为 p 的域即可), 不论开始时选择的 K 是什么, 这个群都同构于 $(\mathbf{Z}/p\mathbf{Z})^2$. 既然这个群对于所有的椭圆曲线都是一样的, 为什么这个群有意思呢? 因为结果是*伽罗瓦群*[V.21] $\mathrm{Gal}(\tilde{K}/K)$ 能够排列集合 $E(\tilde{K})[p]$. 事实上, $\mathrm{Gal}(\tilde{K}/K)$ 在群 $(\mathbf{Z}/p\mathbf{Z})^2$ 上的作用, 给出伽罗瓦群的一个*表示*[III.77]. 这是**伽罗瓦表示理论**的基础性的例子, 而这个理论又是现代数论的中心. 其实怀尔斯 (Andrew Wiles) 对于*费马大定理*[V.10] 的证明说到底就是关于来自椭圆曲线的伽罗瓦表示的一个定理. 而他对于这个特殊的伽罗瓦表示所证明的, 无非就是一大族猜想 (即所谓**朗兰茨纲领**) 的一个特例, 这个纲领提出了伽罗瓦表示和**自守形式**有一个彻底的对应, 而后者就是称为*模形式*[III.59] 的解析函数的推广.

在另一个方向上, 如果 E 是复数域 $\mathbf{C}$ 上的椭圆曲线, 则 E 上具有复坐标的点的集合, 记作 $E(\mathbf{C})$, 构成一个*复流形*[III.88]. 因此, 这个复流形总可以表示为复平面关于某个复变换群 Λ 的商. 更有甚者, 这些复变换就是平移: 每一个变换各把 z 点映为 $z+c$, c 是一个复数, [由这个变换决定] (这里说的把 $E(\mathbf{C})$ 用商来表示, 是由*椭圆函数*[V.31] 来实现的). 这样, 每一个椭圆曲线生成复数的一个子集合 —— 其实是一个子群 —— 这个子群的元素称为椭圆曲线的**周期**. 这个构造方法可以看成是*霍奇*[VI.90] 理论的最初的起点, 这是代数几何以艰深著称的一个分支 (这个理论的一个中心问题, **霍奇猜想**正是 Clay 研究所以百万美元悬赏征解的 7 个问题之一).

由椭圆曲线的*模空间*[IV.8] $M_{1,1}$ 还提出了另一个观点. $M_{1,1}$ 也是一条曲线, 但不是椭圆曲线 (说真的, 如果要我说实话, 我就要说 $M_{1,1}$ 连曲线也不是, 它是一个对象, 其名称可谓是人言人殊: 有人叫它*轨道流形*[IV.4 §7], 有人叫它代数栈 —— 可以把它设想成一条曲线, 但是有人从曲线上面取走了一些点, 并且把这些点或者对半折叠, 或者折叠成三层, 再把这些叠起来的点又粘回原处. 您要是知道, 哪怕这个分支的专家也觉得难以把它弄清楚, 这也算一点安慰吧!) 从两个方面来讲, 曲线 $M_{1,1}$ 都是"最简单的例子": 它是最简单的模曲线, 同时又是曲线的最简单的模空间.

III.22 欧几里得算法和连分数 (The Euclidean Algorithm and Continued Fractions)

Keith Ball

1. 欧几里得算法

算术的基本定理[V.14]是人们在很久远的古代就已经知道的. 通常的证明是依靠所谓欧几里得算法来构造出两个 [正] 整数 m 和 n 的最大公因数 (以下简记为

hcd), 设为 h. 欧几里得算法在做这件事情的时候是证明了 h 可以写成 $am+bn$ 的形式, 这里 a , b 是一对整数 (不一定为正整数, [甚至可以为 0]). 例如, 17 和 7 的 hcd 是 1, 完全肯定我们可以把 1 写成 $1=5\times 17-12\times 7$.

欧几里得算法是这样执行的. 设 $m>n$ [(如果 $m=n$, 则它们的 hcd 就是 m, 而 $m=1\times m+0\times n$, $a=1$,$b=0$.)], 先用 n 去除 m, 得出商为 q_1 而余数为 r_1, 所以

$$m=q_1n+r_1\,. \tag{1}$$

现在 $0\leqslant r_1<n$, 所以又可以用 r_1 去除 n, 得到第二个商和余数:

$$n=q_2r_1+r_2\,. \tag{2}$$

可以这样做下去: 用 r_2 去除 r_1, 用 r_3 去除 r_2, 等等. 余数每一次都会变小, 但是因为它不会是负数, 所以到了某一步余数就会变成 0, 就是除尽了. 例如, 如果 $m=165$, $n=70$, 这个算法就会给出一系列除法如下:

$$165=2\times 70+25\,, \tag{3}$$

$$70=2\times 25+20\,, \tag{4}$$

$$25=1\times 20+5\,, \tag{5}$$

$$20=4\times 5+0\,. \tag{6}$$

这个过程保证了最后一个非零的余数就是 m 和 n 的 hcd. 现在它等于 5. [其理由如下:] 一方面, 式 (6) 说明了 5 是前一个余数 20 的因数, 再往上看式 (5), 又说明 5 也是 25 的因数, 因为 25 是表示为 20 和 5 的组合. 这样一直往上看, 这个算法告诉我们 5 同时是 $m=165$ 和 $n=70$ 的因数, 所以 5 是它们的公因数.

另一方面, 倒数第二式 (5) 说明 5 可以写成 25 和 20 的组合, 而且系数是整数. 再往上看式 (4), 20 又可以写成 70 和 25 的组合, 所以 5 也可以写成 70 和 25 的组合

$$5=25-20=25-(70-2\times 25)=3\times 25-70\,.$$

仿此倒推这个算法, 可以把 25 用 165 和 70 表示为

$$5=3\times(165-2\times 70)-70=3\times 165-7\times 70\,.$$

这就说明 5 是 165 和 70 的**最大公因数**, 因为由上式可知 165 和 70 的任意的公因数都必然是 $3\times 165-7\times 70$ 的因数, 即 5 的因数. 沿着这样的道路, 我们已经证明了最大公因数一定可以用两个原来的数 m 和 n 来表示.

2. 用连分数表示数

在欧几里得以后的 1500 年间, 伊斯兰和印度学派的数学家们认识到, 欧几里得算法对于一对整数 m 和 n 的执行过程可以用比 m/n 的一个公式来记. 方程式 (1) 可以写为

$$\frac{m}{n} = q_1 + \frac{r_1}{n} = q_1 + \frac{1}{F},$$

这里 $F = n/r_1$. 现在 (2) 式又把 F 写成

$$F = q_2 + \frac{r_2}{r_1}.$$

再往下一步就会给出 [r_2/r_1 的倒数]r_1/r_2 的一个表达式, [把它表示为一个整数 (就是商) 和一个真分数 (后一个余数与前一个余数之比) 的和]. 仿此以往, 如果这个算法在第 k 步停了下来, 我们就把这些表达式放在一起, 得到 m/n 的**连分数表达式**:

$$\frac{m}{n} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ddots + \cfrac{1}{q_k}}},$$

例如

$$\frac{165}{70} = 2 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{4}}}.$$

连分数也可以直接从分数 165/70=2.35714··· 做出来, 而不必用到两个整数 165 和 70. 实际上, 取这个数的整数部分 2, [这就是前面的 q_1]. 再把余下的小数部分取其倒数 $1/0.35714\cdots = 2.8$, 又取其整数部分 2, 就得到前面的 q_2. 余下的 0.8 倒数为 1.25, 所以 $q_3 = 1$. 最后 $1/0.25 = 4$, 所以 $q_4 = 4$. 至此, 余数为 0, 而运算停止.

17 世纪的数学家沃利斯 (John Wallis, 1616 –1703, 英国数学家) 似乎是第一个给出了连分数的系统讨论的数学家, 而且似乎是第一个认识到, 不仅是有理数, 而且是所有实数都有连分数展开式存在的人, 只要我们承认连分数可以有无限多层. 如果从任意正数开始, 都可以像对付比值 2.35714··· 一样地构造出连分数来. 例如对于数 $\pi = 3.14159265\cdots$, 先取 3, 再把余下的部分取倒数: $1/0.14159\cdots =$

7.06251⋯. 这样对于 π 第二个商是 7. 继续这样做下去, 就得到连分数

$$\pi = 3 + \cfrac{1}{7 + \cfrac{1}{15 + \cfrac{1}{1 + \cfrac{1}{292 + \cfrac{1}{1 + \ddots}}}}}. \tag{7}$$

出现在分数里的 3, 7, 15 等就叫做 π 的**部分商**.

实数的连分数表达式可以用来求此实数的有理数近似. 如果把这个连分数在有限步以后就截断, 就会得到一个有限的连分数. 它是一个有理数. 例如, 把 (7) 式在第一层就截断, 就会得到我们熟知的 π 的近似值: $3+\frac{1}{7}=\frac{22}{7}$; 在第二层截断又会得到 π 的另一个近似值: $3+1/(7+1/15)=333/106$. 在不同的层截断就会得出一个有理逼近序列, 它的前一部分是

$$3,\ 22/7,\ 333/106,\ 355/113,\ \cdots$$ [①]

不论从哪一个正实数 x 开始, 它的连分数逼近的序列当沿连分数的各层向下走的时候都将趋近 x. 事实上, 等式 (7) 的形式解释就是说, 它的不同层面的截断会趋近 π .

很自然地, 想要得到数 x 的更好的近似, 就应该用 "更复杂" 的分数 —— 就是具有更大的分子和分母的分数. x 的连分数逼近在下面的意义上是最好的逼近: 若 p/q 是这个连分数的一个截断, 则不可能找到分母小于 q 的分数 r/s 与 x 更加接近.

进一步说, 如果 p/q 是来自连分数的对 x 的逼近, 则 $\left|x-\frac{p}{q}\right|$ 相对于分母 q 不能太大. 具体说来, 恒有

$$\left|x-\frac{p}{q}\right| \leqslant \frac{1}{q^2}. \tag{8}$$

这个误差估计说明了连分数近似是多么特别, 如果想也不想地取一个分母 q, 然后又想也不想地取一个分子 p 并且希望用 p/q 去逼近 x, 那么只能保证 x 位于 $(p-1/2)/q$ 和 $(p+1/2)/q$ 之间, 所以误差可能达到 $1/2q$, 而当 q 很大时, 这可比 $1/q^2$ 大多了.

有时, x 的连分数近似的误差比 (8) 式所保证的还要小, 即如通过对 (7) 式作截断所得到的近似 $\pi \approx 335/113$ 就特别精确. 原因在于下一个部分商 292 很大, 所以略去尾巴 $1/\left(292+1/\left(1+\ddots\right)\right)$ 并不会造成大的改变. 在这个意义下, 最难用

①祖冲之的疏率和密率都在这个序列中.—— 中译本注

连分数去逼近的数是部分商最小的数也就是所有部分商都等于 1 的数. 这个数

$$1+\cfrac{1}{1+\cfrac{1}{1+\ddots}} \tag{9}$$

很容易计算, 因为其部分商序列是周期的. 若记此数为 ϕ, 则 $\phi-1=1/\left(1+1/\left(1+\ddots\right)\right)$, 而它的倒数就是 (9) 式的连分数 ϕ. 所以

$$\frac{1}{\phi-1}=\phi,$$

也就是 $\phi^2-\phi=1$. 这个二次方程式的两个根是 $(1+\sqrt{5})/2=1.518\cdots$ 和 $(1-\sqrt{5})/2=-0.618\cdots$. 因为我们想要找的数 φ 是正的, 所以它就是第一个根, 就是常说的**黄金比**(或**黄金分割**).

很容易看到, 正如 (9) 表示的是正根, 其他的周期连分数也表示某个二次方程式的根. 这件事, 似乎在 16 世纪就已为人所理解了. 但是要想证明其逆可就难多了, 任意二次根的连分数必为周期的. 直到 18 世纪拉格朗日[VI.22] 才证明了它, 而这与二次数域[III.63] 有单位元存在有密切的关系.

3. 用连分数表示函数

数学最重要的函数中有几个用无穷和来表示最为容易. 例如, 指数函数[III.25] 就有以下的无穷级数表示:

$$\mathrm{e}^x=1+x+\frac{x^2}{2!}+\cdots+\frac{x^n}{n!}+\cdots.$$

但是也有几个有简单的连分数表示, 就是用含有变量如 x 的连分数来表示. 从历史上来说, 这些可能是最重要的连分数.

例如, 函数 $x\mapsto\tan x$ 就有以下的连分数表示:

$$\tan x=\cfrac{x}{1-\cfrac{x^2}{3-\cfrac{x^2}{5-\ddots}}}, \tag{10}$$

它对除了 $\pi/2$ 的奇数倍以外的 x 都适用, 在这些点处正切函数有垂直的渐近线.

一个函数的无穷级数表示可以提供这个函数的多项式逼近, 而连分数在截断后则提供了这个函数的有理函数 (即多项式之商) 逼近. 例如, 如果把正切函数的连分数表示在第一层截断, 就会得到以下近似

$$\tan x=\frac{x}{1-x^2/3}=\frac{3x}{3-x^2}.$$

这个连分数表示以及它在截断以后逼近 $\tan x$ 的速度, 在证明 π 为无理数 (即不是两个整数之比) 上起着中心的作用. 这个证明是由兰伯特 (Johann Heinrich Lambert, 1728–1777, 瑞士数学家) 在 1760 年代给出的. 他用连分数证明了若 x 是除 0 以外的有理数, 则 $\tan x$ 不是. 但是 $\tan\pi/4=1$ 肯定是有理数, 所以 $\pi/4$ 不可能是有理数.

III.23 欧拉方程和纳维–斯托克斯方程 (The Euler and Navier-Stokes Equations)

Charles Fefferman

欧拉方程是描述理想流体 (即没有粘性的流体) 运动的基本的方程, 而纳维–斯托克斯方程则是描述有粘性的流体运动的基本方程, 以下简记为 N-S 方程 (纳维 (Claude-Louis Navier), 1785–1836, 法国工程师和力学家; 斯托克斯 (Sir George Gabriel Stokes), 1819–1903, 英国数学物理学家)①这些方程在科学和工程上都是重要的, 然而人们对它们的了解还很不够. 它们是对数学的重大挑战.

为了描述这些方程, 我们在欧几里得空间 $\mathbf{R}^d$ 中进行研究, 这里 d 表示维数, 是 2 或者 3. 设在点 $x=(x_1,\cdots,x_d)\in\mathbf{R}^d$ 处, 以及时间 $t\in\mathbf{R}$ 时刻, 流体具有速度向量 $u(x,t)=(u_1(x,t),\cdots,u_d(x,t))\in\mathbf{R}^d$. 流体的压强则是 $p(x,t)\in\mathbf{R}$. 欧拉方程就是对于所有 (x,t),

$$\left(\frac{\partial}{\partial t}+\sum_{j=1}^{d}u_j\frac{\partial}{\partial x_j}\right)u_i(x,t)=-\frac{\partial p}{\partial x_i}(x,t),\quad i=1,\cdots,d. \tag{1}$$

而 N-S 方程则是对于所有 (x,t),

$$\left(\frac{\partial}{\partial t}+\sum_{j=1}^{d}u_j\frac{\partial}{\partial x_j}\right)u_i(x,t)=\nu\left(\sum_{j=1}^{d}\frac{\partial^2}{\partial x_j^2}\right)u_i(x,t)-\frac{\partial p}{\partial x_i}(x,t),\quad i=1,\cdots,d, \tag{2}$$

这里 $\nu>0$ 是一个摩擦系数, 称为流体的 "粘性".

本文中限于讨论不可压缩流体, 就是说, 除了要求适合方程 (1) 或 (2) 以外, 还要求对于一切 (x,t) 适合

$$\operatorname{div}u\equiv\sum_{i=1}^{d}\frac{\partial u_i}{\partial x_i}=0. \tag{3}$$

①这一段原书有明显的疏忽, 即认为纳维–斯托克斯方程也是讲的理想流体, 但是后面又说其中有粘性. 理想流体就是没有粘性的流体, 所以有了矛盾. 现在改写如上. —— 中译本注

欧拉方程和 N-S 方程只不过就是把牛顿定律 $F = ma$ 应用于流体的无穷小部分而已. 事实上, 很容易看到向量

$$\left(\frac{\partial}{\partial t} + \sum_{j=1}^{d} u_j \frac{\partial}{\partial x_j}\right) u$$

就是流体的微元①在位置 x 时刻 t 所经历的加速度.

在欧拉方程中, 牛顿运动定律 $F = ma$ 里的力 F 完全来自压强梯度 (举例来说, 如果压强随高度增加, 则负梯度 $-\mathrm{grad}p = -\left(\frac{\partial p}{\partial x_1}, \cdots, \frac{\partial p}{\partial x_d}\right)$ 指向下方, 所以有一个净力驱使流体向下运动), 但在 N-S 方程 (2) 中还有一个附加项

$$\nu\left(\sum_{j=1}^{d} \frac{\partial^2}{\partial x_j^2}\right) u$$

来自摩擦力.

N-S 方程在许多各种各样的情况下都与对实际流体进行的实验十分符合. 因为流体是很重要的, 所以 N-S 方程也是很重要的.

欧拉方程只不过是 N-S 方程在 $\nu = 0$ 时的极限情况, 但是我们将会看到, 二者的解的性态很不相同, 哪怕是 ν 很小时也是.

我们想要了解在初始条件, 即对于所有 $x \in \mathbf{R}^d$,

$$u(x, 0) = u^0(x) \tag{4}$$

下, 欧拉方程和 (3) 的解或者 N-S 方程和 (3) 的解, 这里 $u^0(x)$ 是已给的初速度. 为了与 (3) 式相容, 假设对于所有 $x \in \mathbf{R}^d$,

$$\mathrm{div} u^0(x) = 0.$$

还有为了避免在物理上不合理的情况, 例如无穷能量, 还假设当 $|x| \to \infty$ 时, $u^0(x)$ 以及具有固定的 t 的 $u(x, t)$ 都 “足够快” 地趋于零. 这里不解释 “足够快” 的确切意义是什么, 但是从现在起就假设只讨论这种急速衰减的速度.

物理学家和工程师想要知道怎样有效而又快速地计算 N-S 方程 (2) 和 (4) 的解, 并理解这些解的性态. 数学家首先要问的是是否有解存在, 如果有, 又是否只有一个解. 虽然欧拉方程已经有了 250 年的历史, N-S 方程的历史也有了 100 年以上, 专家们对于 N-S 方程或者欧拉方程的解是否对于所有时间都存在, 或者会发生 “破裂”, 仍然没有共识. 有严格证明支持的肯定的答案似乎还很遥远.

①原书作 “流体分子” 不妥, 因为这些方程的基本假设是在连续介质观点下讨论流体, 所以必定是不考虑分子观点的, 因此我采用了现在通用的说法, 用 “微元” 代替 “分子”. —— 中译本注

让我们把关于欧拉方程和 N-S 方程的 "破裂问题" 讲得更明确一点. 方程 (1)–(3) 涉及了 $u(x, t)$ 的一阶和二阶导数. 假设 (4) 中的初始速度 $u^0(x)$ 具有一切阶数的导数

$$\partial^\alpha u^0(x) = \left(\frac{\partial}{\partial x_1}\right)^{\alpha_1} \cdots \left(\frac{\partial}{\partial x_d}\right)^{\alpha_d} u^0(x),$$

而且当 $|x| \to \infty$ 时, 它们都 "足够快" 地趋于零, 这些都是很自然的. 于是我们要问, 是否 N-S 方程 (2)–(4) 或者欧拉方程 (1), (3) 和 (4) 对于所有的 $x \in \mathbf{R}^d$ 和 $t > 0$ 都有解 $u(x, t)$ 和 $p(x, t)$, 使得对于所有的 $x \in \mathbf{R}^d$ 和 $t > 0$, 导数

$$\partial^\alpha_{x,t} u(x, t) = \left(\frac{\partial}{\partial t}\right)^{\alpha_0} \left(\frac{\partial}{\partial x_1}\right)^{\alpha_1} \cdots \left(\frac{\partial}{\partial x_d}\right)^{\alpha_d} u(x, t)$$

和 $\partial^\alpha_{x,t} p(x, t)$ 都存在 (而且当 $|x| \to \infty$ 时, 都 "足够快" 地趋于零). 具有这种性质的一对 u 和 p 称为欧拉方程或 N-S 方程的 "光滑解". 谁也不知道 (在 3 维情况下) 这种解是否存在. 我们知道有某个依赖于初始速度 (4) 的正的时刻 $T = T(u^0) > 0$, 使得欧拉方程或 N-S 方程有 "光滑解" 在 $x \in \mathbf{R}^d$, $t \in [0, T)$ 中存在.

在 2 维空间情况 (这时我们说 2D 欧拉或 2D N-S), 可以取 $T = +\infty$, 就是说对于 2D 欧拉或 2D N-S 不会发生 "破裂". 在 3 维空间的情况, 谁也不能排除有这样的可能: 对于某个如上所述的 $T = T(u^0)$, 可以在区域

$$\Omega = \left\{(x, t) : x \in \mathbf{R}^d, t \in [0, T)\right\}$$

中找到欧拉方程或 N-S 方程的解 $u(x, t)$, $p(x, t)$, 它在此区域中光滑, 但是有一个导数使得 $\left|\partial^\alpha_{x,t} u(x, t)\right|$ 或 $\left|\partial^\alpha_{x,t} p(x, t)\right|$ 在其中无界. 这将意味着在越过时刻 T 以后就不会有光滑解了 (我们就说 3D 欧拉或 3D N-S 在时刻 T 破裂). 说不定对于 3D 欧拉以及/或者 3D N-S 真就发生了这样的事情, 谁也不知道相信什么才好.

对于 3D N-S 以及 3D 欧拉, 人们已经做出过不少计算机仿真. 纳维–斯托克斯的仿真并没有显示出有破裂的证据, 但是这可能只意味着会产生破裂的初速度 u^0 极为罕见. 3D 欧拉的形态可能极为狂野, 所以很难判断一项给定的数值研究是否表示发生了破裂. 事实上, 要完成一项可靠的 3D 欧拉的数值仿真, 是难得出了名的事.

假设会发生破裂, 并且研究这时 N-S 方程或欧拉方程解的性态, 这是很有用的. 例如设在时刻 $T < \infty$ 对于 3D 欧拉发生了破裂, Beale, Kato 和 Majda 有一个定理断言, 当 $t \to T$ 时 "涡度"

$$\omega(x, t) = \operatorname{curl}(u(x, t)) = \left(\frac{\partial u_2}{\partial x_3} - \frac{\partial u_3}{\partial x_2}, \frac{\partial u_3}{\partial x_1} - \frac{\partial u_1}{\partial x_3}, \frac{\partial u_1}{\partial x_2} - \frac{\partial u_2}{\partial x_1}\right) \tag{5}$$

会增长得这样快, 使得积分

$$\int_0^T \left(\max_{x\in\mathbf{R}^d}|\omega(x,t)|\right)\mathrm{d}t$$

发散. 这件事被用来指明某些声称证明了 3D 欧拉发生了破裂的计算机仿真其实是无效的. 现在也知道当 t 接近一个有限的破裂时刻 T 时, 涡度向量的方向会随着 x 的变化而狂野地变动.

(5) 式的向量 ω 有很自然的物理意义: 它表示在时刻 t 流体怎样绕着 x 点旋转. 如果在 x 点处, 在时刻 t, 放一个小涡轮, 使它的轴的定向平行于 $\omega(x,t)$, 则这个涡轮会被流体以角速度 $|\omega(x,t)|$ 旋转起来.

对于 3D N-S, Sverak 最近有一个结果说, 如果发生了破裂, 则压强 $p(x,t)$ 上下方均为无界.

1930 年代, 由勒雷 (Jean Leray, 1906–1998, 法国数学家) 首创地提出了一个非常有前途的思想: 研究 N-S 方程的 "弱解". 他的思想如下: 初看起来, N-S 方程 (2) 和 (3) 只有当 $u(x,t)$ 和 $p(x,t)$ 为充分光滑时才有意义, 例如, 我们可能希望 u 对 x_j 具有 2 阶导数, [因为这种导数出现在 (2) 式的右方]. 然而, 如果做形式的运算就会发现, (2) 和 (3) 等价于下面的 (2′) 和 (3′), 而在那里, 即令 $u(x,t)$, $p(x,t)$ 很粗糙, 也是有意义的. 让我们先来看一下 (2′) 和 (3′) 是怎样导出来的, 然后再来看它们的用处.

起点是以下的观察: $\mathbf{R}^n$ 上的一个函数 F 恒等于零当且仅当对于每一个光滑的 [且在某一紧集合外恒为 0 的函数][①] θ 都有 $\int_{\mathbf{R}^n}F\theta\mathrm{d}x=0$. 把这一点说明用于方程 (2) 和 (3), 再作一点形式运算 (即分部积分) 就知道它们等价于

$$\iint_{\mathbf{R}^3\times(0,\infty)}\left\{-\sum_{i=1}^3 u_i\frac{\partial\theta_i}{\partial t}-\sum_{i,j=1}^3 u_iu_j\left(\frac{\partial\theta_i}{\partial x_j}\right)\right\}\mathrm{d}x\mathrm{d}t$$

$$=\iint_{\mathbf{R}^3\times(0,\infty)}\left\{\nu\sum_{i,j=1}^3\left(\frac{\partial^2}{\partial x_j^2}\theta_i\right)u_i+\left(\sum_{i=1}^3\frac{\partial\theta_i}{\partial x_i}\right)p\right\}\mathrm{d}x\mathrm{d}t, \tag{2′}$$

以及

$$\iint_{\mathbf{R}^3\times(0,\infty)}\left\{\sum_{i=1}^3 u_i\frac{\partial\phi}{\partial x_i}\right\}\mathrm{d}x\mathrm{d}t=0. \tag{3′}$$

更准确地说, 给定任意的光滑的函数 $u(x,t)$ 和 $p(x,t)$, 方程 (2) 和 (3) 成立的充分必要条件是 (2′), (3′) 对于任意光滑而且在 $\mathbf{R}^3\times(0,\infty)$ 的某个紧集合外恒为 0 的函数 $\theta_1(x,t)$, $\theta_2(x,t)$, $\theta_3(x,t)$ 和 $\varphi(x,t)$ 均成立.

①原书在这里有疏忽. —— 中译本注

称函数 $\theta_1(x, t)$, $\theta_2(x, t)$, $\theta_3(x, t)$ 和 $\varphi(x, t)$ 为**试验函数**, 而说 u 和 p 是 3D N-S 的**弱解**. 因为在 (2′), (3′) 中, 所有的导数都是对于光滑的试验函数取的, 所以它们对于很粗糙的函数 $u(x, t)$ 和 $p(x, t)$ 仍是有意义的. 总结起来, 我们有如下的结论:

一对光滑的(u, p)解出了 3D N-S 当且仅当它们是弱解. 然而弱解的思想即令对于粗糙的(u, p)也是有意义的.

我们希望能按以下的步骤来应用弱解:

步骤 (i): 证明 3D N-S 在整个 $\mathbf{R}^3 \times (0, \infty)$ 上有适当的弱解存在.

步骤 (ii): 证明 3D N-S 的任意适当的弱解必定是光滑的.

步骤 (iii): 由此得到结论, 在步骤 (i) 中做出的适当弱解就是 3D N-S 在整个 $\mathbf{R}^3 \times (0, \infty)$ 上的光滑解.

在这里 "适当的" 就是指 "不太大的", 它的精确定义我们就略过不说了.

上面的计划对于某些有趣的偏微分方程是成功的, 但是对于 3D N-S, 这个计划只部分地实现了. 很久以来人们就知道如何构造出 3D N-S 的适当的弱解, 但是其唯一性一直没有得到证明. 感谢 Sheffer, Lin, Caffarelli, Kohn 和 Nirenberg 等人的工作, 现在已经知道了, 在一个具有小的*分形维数*[III.17] 的集合 $E \subset \mathbf{R}^3 \times (0, \infty)$ 之外, 3D N-S 的任一适当的弱解都是光滑的 (即必定具有任意阶的导数). 特别是 E 中不会包含曲线. 要想排除破裂, 就必须证明 E 是空集合.

对于欧拉方程, 弱解仍是有意义的, 但是 Sheffer 和 Schnirelman 举出的例子表明, 它们的性态可能很奇怪. 一个 2 维的流体在开始可能是平静的, 后来不受任何外力的作用却突然在一个有界的空间区域里运动起来, 然后又恢复平静. 对于 2D 欧拉的弱解, 这种行为可能会发生的.

除了上面讲过了的破裂问题以外, 纳维–斯托克斯和欧拉方程还会引起一些其他的基本问题. 我们现在再讲一个这样的问题来结束本文. 设固定了 3D N-S 或 3D 欧拉的初始值 $u^0(x)$, 则在时刻 $t=0$ 的能量是

$$E_0 = \frac{1}{2}\int_{\mathbf{R}^3} |u(x, 0)|\, \mathrm{d}x .$$

对于 $\nu \geqslant 0$, 用 $u^{(\nu)}(x, t) = \left(u_1^{(\nu)}, u_2^{(\nu)}, u_3^{(\nu)}\right)$ 来表示以 $u^0(x)$ 为初速度, 粘性为 ν 的 3D N-S 的解 (若 $\nu = 0$ 则 $u^{(0)}(x, t)$ 是欧拉方程的解). 假设 $u^{(\nu)}$ 在一切时间都存在 (至少当 $\nu > 0$ 时如此). 则在 $t \geqslant 0$ 时, $u^{(\nu)}(x, t)$ 的能量是

$$E^{(\nu)}(t) = \frac{1}{2}\int_{\mathbf{R}^3} \left|u^{(\nu)}(x, t)\right|^2 \mathrm{d}x .$$

以 (1)–(3) 为基础作一些初等的运算 (以 u_i 遍乘 (1) 或者 (2), 对 i 求和, 对 $x \in \mathbf{R}^3$

积分, 再作分部积分) 即得

$$\frac{\mathrm{d}}{\mathrm{d}t}E^{(\nu)}(t)=-\frac{1}{2}\nu\int_{\mathbf{R}^3}\sum_{i,j=1}^{3}\left(\frac{\partial u_i^{(\nu)}}{\partial x_j}\right)^2\mathrm{d}x. \tag{6}$$

特别是对于欧拉方程有 $\nu=0$, 因此 (6) 式给出, 能量等于一个常数 E_0, 而只要解是存在的, 它就与时间无关.

现在假设 ν 很小, 但不是零. 由 (6) 式自然会猜想, 当 ν 很小时, $|(\mathrm{d}/\mathrm{d}t)E^{(\nu)}(t)|$ 也很小, 所以在很长的时间段里几乎是常数. 然而数值试验和物理实验都强烈地指出并不如此. 相反, 似乎存在一个依赖于 u^0 但是与 ν 无关的 $T_0>0$, 使得流体的初始能量到了时刻 T_0 至少损失一半, 而不论 ν 多么小 (当然要 $\nu>0$).

如果能够证明或否定这个结论是很重要的. 我们需要理解, 为什么这么小的粘性会产生如此大的能量耗散.

III.24 伸展图
(Avi Wigderson)

1. 基本定义

一个伸展图 (expander) 就是一种特殊的图[III.34], 它有值得注意的性质和许多应用. 粗略地说, 它是一个很难切断的图, 因为它的顶点的任一集合都有许多边, 把这个集合和顶点集合在此图中的余集合连接起来. 更准确地说, 一个 c- 伸展图就是这样一个具有 n 个顶点的图, 如果对于顶点集合的每一个 m 点子集合 S(这里 $m\leqslant\frac{1}{2}n$), 至少有 cm 条边把 S 和 S 的余集合连接起来.

当图 G 很稀疏时, 即当此图的边很少的时候, 这个定义特别有意义. 我们将要集中注意一个重要的特例, 即 G 为**一度数为 d 的正规图**的情况, 这里 d 是一个固定常数, 而且与 n 无关, 这就是说, 每一个顶点恰好与 d 个其他顶点连接. 当 G 是度数为 d 的正规图时, 由 S 到 S 的余集合的边数最多显然为 dm, 所以, 如果 c 是某个固定常数 (即不随 n 趋于零的常数), 则在顶点的任意子集合与其余集合之间的边数总在最大边数的一定倍数之内. 这个评论提示我们, 不仅要关心的单个的图, 而且要关心图的无穷的族, 我们说一个无穷族的 d- 正规图, 是**一族**伸展图, 如果存在一个常数 $c>0$, 使得这个族中的每一个图都是一个 c- 伸展图.

2. 伸展图的存在性

第一个证明伸展图存在的人是 Pinsker, 他证明了如果 n 很大, 而 $d\geqslant 3$, 则几乎每一个具有 n 个顶点的图都是一个伸展图. 即他证明了存在一个常数 $c>0$, 使

得对于每一个固定的 $d \geqslant 3$, 具有 n 个顶点的 d- 正规图中, 不是伸展图的那一部分所占的比随 $n \to \infty$ 而趋于零. 这个证明是组合学的概率方法[IV.19 §3] 的一个早期的例子. 不难看到, 如果均匀地随机选取一个 d- 正规图, 则离开集合 S 的边的数目的期望值是 $d|S|(n-|S|)/n$, 它最少是 $\left(\frac{1}{2}d\right)|S|$. 用标准的 "正反面估计" 可以证明, 对于固定的 S, 离开 S 的边数显著地与这个期望值不同的概率是极小的, 小到甚至把所有集合的概率加起来仍然很小. 所以, 所有的集合 S 至少有 $c|S|$ 条边连接到其余集合的概率是很大的 (从一个方面看来, 这样的描述有些误导: 要讨论关于随机的 d- 正规图的事件的概率并不是一件直截了当的事, 因为这些边的选取并不是独立事件, 然而 Bollobás 定义了随机 d- 正规图的一个等价的模型, 在其中可以这样来处理这个问题).

注意, 这个证明并没有给我们以任何伸展图的显式的描述: 它只是证明了伸展图大量存在. 这是这个证明的缺点, 因为我们将会看到, 伸展图有许多应用是依赖于某种显式的描述的, 至少是依赖于生成伸展图的有效的方法. 但是 "显式的描述" 或者 "有效的方法" 确切地何所指? 对于这个问题可以有许多答案, 我们只来讨论两个. 第一个是要求有一个算法, 对于任意的整数 n, 在关于 n 为多项式的时间内, 列举出具有大约 n 个顶点 (或者灵活一点, 要求顶点的数目在 n 和 n^2 之间) 的 d-正规 c- 伸展图的所有的顶点和边 (关于多项式时间可参见计算复杂性[IV.20§2]). 这种类型的描述, 有时称为 "适度显式" 的描述.

为了对于所谓 "适度" 有一点概念, 考虑下面的图. 它的顶点都是长为 k 的 01 序列, 如果两个顶点只在一个位数上不同, 就认为它们是由一个边连接起来的. 这个图有时称为**离散的 k 维立方体**. 它有 2^k 个顶点, 所以想要列举出它的顶点和边所需的时间是巨大的. 然而对于许多目的, 我们并不真正需要这样一个清单, 真正起作用的是需要有一个简明的方法来表示每一个顶点, 有一个有效的算法来列举出与任一个顶点相连接的顶点 (有了这种连接的顶点的一种表示). 01 序列本身就是一种简明的表示, 而在给出了一个 01 序列 σ 以后, 很容易就可以在 k 的多项式时间而不是在 2^k 时间内列出与这个顶点相连接的 k 个顶点: 每一次只需把 σ 的某一位数从 0 变成 1, 或者从 1 变成 0 即可. 可以像这样有效地描述的图 (列出连接的顶点只需要顶点数的对数的多项式时间) 称为**强显式的**.

对于可以显式构造的伸展图的探求是许多美丽的数学的起源, 这种探求时常要用到来自数论和代数这些领域的思想. 第一个显式伸展图是由 Margulis 发现的. 我们要给出他的作法和另一个构造的实例. 我们要强调, 虽然这些作法描述起来很简单, 但是要证明它们确实是伸展图就远没有这么容易了.

Marguli 构造的伸展图是对于任意整数 m 作出一个 8- 正规图 G_m 如下: 它的顶点集合是 $\mathbf{Z}_m \times \mathbf{Z}_m$, $\mathbf{Z}_m$ 是所有整数 mod m 的集合; 与顶点 (x, y) 连接的顶点

是以下 8 个点:

$$(x+y\ ,\ y)\ ,\ (x-y\ ,\ y)\ ,\ (x\ ,\ y+x)\ ,\ (x\ ,\ y-x)\ ,$$
$$(x+y+1\ ,\ y)\ ,\ (x-y+1\ ,\ y)\ ,\ (x\ ,\ y+x+1)\ ,\ (x\ ,\ y-x+1)$$

(所有的运算都是在 mod m 意义下进行的). Margulis 对于 G_m 是一个伸展图的证明是基于*表示理论*[IV.9] 的, 而对膨胀常数 c 并没有给出确定的界限. 后来, Gabber 和 Galil 又用*调和分析*[IV.11] 导出了这样一个界限.

另一个构造的实例是对每一个素数 p 作出一个具有 p 个顶点的 3- 正规图. 这一次, 顶点集合是 $\mathbf{Z}_p$, 而与顶点连接的顶点是 $x-1$, $x+1$ 和 x^{-1}(这是指 x 在 mod p 意义下的逆元, 0 的逆元则定义为 0). 这些图是伸展图的证明依赖于数论中的一个深刻的结果, 称为塞尔贝格 3/16 定理. 这一族图只是适度显式的.

直到最近, 显式构造伸展图的方法都是代数方法. 然而, 在 2002 年, Reingold, Vadhan 和 Wigderson 引入了图的所谓锯齿积, 用它给出了构造伸展图的一种组合的迭代方法.

3. 伸展图和本征值

一个图成为 c- 伸展图的条件牵涉到图的所有的顶点之集合的子集合. 因为子集合的个数是指数多的, 所以从表面上看来, 验证一个图是否为 c- 伸展图是一个指数长时间的任务. 事实上, 这个问题是一个 *$\mathcal{CO}$-$\mathcal{NP}$完全问题*[IV.20 §§3,4]. 然而我们现在要描述一个密切相关的性质, 而此限制可以在多项式时间内验证, 这样它就比较自然了.

设给定了一个具有 n 个顶点的图 G, 它的**连接矩阵** $A=(A_{ij})$ 是一个 $n\times n$ 矩阵, 如果 u 和 v 和相连接的顶点, 就定义其元素 $A_{uv}=1$, 否则就定义 $A_{uv}=0$. 这个矩阵是实对称矩阵, 因此有 n 个*实本征值*[I.3 §4.3]λ_1 , λ_2 , $\cdots$, λ_n. 我们这样来排列这些本征值, 使得 $\lambda_1\geqslant\lambda_2\geqslant\cdots\geqslant\lambda_n$. 此外, 对应于不同本征值的*本征向量*[I.3 §4.3]是互相正交的.

因此, 这些本征值记录了关于 G 的大量信息. 但是在考虑这些事情以前, 我们先来看一下 A 作为一个线性映射是怎样起作用的. 令函数 f 定义在 G 的顶点上, 则 Af 是这样一个函数, 它在顶点 u 上的值等于函数 f 在所有与 u 连接的顶点 v 上的值 $f(v)$ 之和. 由此立即看到, 如果 G 是一个 d- 正规图, 而 f 是在每个顶点上都等于 1 的函数, 则 Af 是在每一个顶点上都等于 d 的函数. 所以常值函数是相应于本征值 d 的本征向量. 也不难看到, 这个本征值是最大的本征值 λ_1, 而如果图 G 是连通的, 则第二大的本征值 λ_2 将严格地小于 d.

事实上, λ_2 与连通性的关系比以上所说的深刻得多, 粗略地说, λ_2 离 d 越远, 图的膨胀参数 c 就越大. 确切一点说, 可以证明 c 在 $\dfrac{1}{2}(d-\lambda_2)$ 和 $\sqrt{2d(d-\lambda_2)}$ 之间.

由此可得, d- 正规图的一个无穷族是一族伸展图, 当且仅当存在某个常数 $a>0$, 使得对于此族的每一个图, **谱间隙** $d-\lambda_2$ 至少是 a . 这些关于 c 的界限之所以重要, 理由之一就在于, 虽然如我们所说, 验证一个图是否 c- 伸展图是很难的事, 其第二大的本征值却可以在多项式时间内计算出来. 所以我们至少能估计出一个图的膨胀性质有多好.

d- 正规图 G 的另一个重要的参数是除 λ_1 以外的任意本征值的最大绝对值. 这个参数记作 $\lambda(G)$. 如果 $\lambda(G)$ 很小, 则 G 的行为很像一个随机的 d- 正规图. 例如, 设 A 和 B 是两个不相交的顶点集合. 如果 G 是随机的, 稍作计算就可以得出, 连接 A 和 B 的边的数目的期望值 $E(A, B)$ 大约是 $d|A||B|/n$. 可以证明, 在任意的 d - 正规图 G 中, $E(A, B)$ 与这个期望值之差最多是 $\lambda(G)\sqrt{|A||B|}$. 所以, 如果 $\lambda(G)$ 只是 d 的很小一部分, 则会得到, 在两个合理大的集合 A 与 B 之间的边数, 大体与我们的期望相同. 这说明, $\lambda(G)$ 很小的图 G, "行为很像是随机图".

自然会问, 在一个 d- 正规图中, $\lambda(G)$ 会多么小. Alon 和 Boppana 证明了它最少总是 $2\sqrt{d-1}-g(n)$, 这里 $g(n)$ 是某个当 n 增加时会趋于 0 的函数. 弗里德曼 (Friedman) 证明了对于几乎所有的具有 n 个顶点的 d - 正规图 G, $\lambda(G)\leqslant 2\sqrt{d-1}+h(n)$, 其中 $h(n)$ 是一个当 n 增加时会趋于 0 的函数, 所以一个典型的 d - 正规图总是很接近匹配于 $\lambda(G)$ 的最佳界限. 这个证明是一项杰作. 更加值得注意的是, 可以把下界与**显式**构造联系起来, 即 Lubotzky, Philips 和 Sarnak 的著名的 Ramanujan 图, Margulis 也独立地得出了这一点. 对于每一个使 $d-1$ 为一个素数之幂的数 d, 他们构造出了一族 $\lambda(G)=2\sqrt{d-1}$ 的 d - 正规图 G.

4. 伸展图的应用

伸展图最明显的应用可能是用于通讯网络. 伸展图的高度连通性意味着这个网络是 "高度容错的", 就是说不可能切除网络的一部分而不破坏大量的通讯线路. 分析伸展图上的随机游动, 还会得出这样的网络的其他让人欢迎的性质, 例如直径很小.

d- 正规图 G 上的长度为 d 的随机游动, 就是一条路径 $v_0, v_1, \cdots, v_m$, 这里每一个 v_i 都是从与其连接的 v_{i-1} 中随机地选出来的. 图上的随机游动可以用于许多现象的模型, 而我们对于随机游动常问的问题是它 "混合" 得有多么快, 就是说 m 要选得多么大, 才能使对于所有顶点 v , $v_m=v$ 的概率近于相同?

如果令 $p_k(v)$ 表示 $v_k=v$ 的概率, 不难证明 $p_{k+1}=d^{-1}Ap_k$. 换句话说, 随机游动的转移矩阵 (transition matrix) T 就是 d^{-1} 乘上连接矩阵, 转移矩阵告诉我们, 在第 $k+1$ 步以后的分布怎样依赖于第 k 步以后的分布. 所以, 转移矩阵最大的本征值为 1, 而当 $\lambda(G)$ 很小时, 所有其他的本征值都很小.

假设现在已经是这个情况, 令 p 为 G 的顶点上的任意概率分布[III.71]. 于是可以把它写成线性组合 $\sum_i u_i$, 这里 u_i 是转移矩阵 T 的相应于本征值 $d^{-1}\lambda_i$ 的本征

向量. 如果把 T 使用 k 次, 就会得到一个新的概率分布 $\sum_i (d^{-1}\lambda_i)^k u_i$. 如果 $\lambda(G)$ 很小, 则 $(d^{-1}\lambda_i)^k$ 除了 $i=1$ 时 $(d^{-1}\lambda_1)^k = 1$ 以外, 其余的很快就趋于 0. 换句话说, 在很短一段时间以后, p 的 "非常数部分" 很快就趋于 0, 而留下的只有均匀分布.

这样, 伸展图上的混合发生得很快. 这个事实是伸展图的许多应用的核心. 例如, 设 V 是一个很大的集合, f 是由 V 到区间 [0, 1] 的函数, 而我们想迅速而又准确地估计 f 的均值. 一个自然的思想是选取 V 中的点的随机样本 $v_1, \cdots, v_k$ 并计算平均值 $k^{-1}\sum_{i=1}^k f(v_i)$. 如果 k 很大, 而 v_i 又是独立地选取的, 则不难证明, 这个样本平均值几乎一定接近于真正的平均值, 它们之差大于 ε 的概率最多是 $e^{-\varepsilon^2 k}$.

这个思想很简单, 但是实行起来需要有随机性的资源. 在理论计算机科学里, 随机性是作为一种资源来看待的, 最好是能够少用就少用. 以上的过程对于每一个 v_i 都需要 $\log(|V|)$bit 的随机性, 所以总共需要 $k\log(|V|)$ bit. 能不能做得更好一点呢? Ajtai, Komlós 和 Szemerédi 证明答案是肯定的, 真了不起! 需要做的只是把 V 和一个伸展图的顶点集合联系起来就行了. 不再需要独立地选取 $v_1, \cdots, v_k$, 只需要把 V 选成这个伸展图图上的随机游动的顶点而以 V 上的随机点 v_1 为出发点就行了. 这时需要的随机性就少多了, 选 v_1 需要 $\log(|V|)$ bit, 而选后面的每一个 v_i 又各需要 $\log(d)$ bit, 所以一共需要 $\log(|V|) + k\log(d)$ bit. 因为 V 很大, 而 d 则是一个固定常数, 所以节省是很大的, 基本上只需为第一个样本点付出成本.

但是这个样本选什么好? 显然 v_i 之间有很大的依赖性. 然而, 可以证明在准确性上**没有**任何损失. 再者, 这个估计与真平均值之差大于 ε 的概率又最多是 $e^{-\varepsilon^2 k}$. 这样在随机性上面的节省, 并没有附加代价.

这只是伸展图的众多应用之一例, 而这些应用既包括实际的应用, 也包括在纯粹数学中的应用. 例如, Gromov 就利用它给出了著名的 Baum-Connes 猜想[IV.15 §4.4] 的某些变体. 而有些被称为 "无损失伸展图" 的二部图又被用于生成具有有效解码的线性编码 (这句话的意思可见信息的可靠传输[VII.6]).

III.25　指数和对数函数

(The Exponential and Logarithmic Functions)

1. 指数化

下面是一个非常著名的数学序列：2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, $\cdots$. 序列中的每一项都是前一项的两倍, 例如, 128, 即序列的第 7 项等于 $2\times2\times2\times2\times2\times2\times2$. 因为这种连乘在整个数学中都出现, 所以采用一个不太冗长的记号是有用的, 这样, 我们通常把它记作 2^7, 读作 "2 的 7 次方". 一般地说, 设 a 是任意实数,

而 m 是任意正整数, 则 a^m 代表 $a\times a\times\cdots\times a$, 其中一共有 m 个 a. a^m 读作 a 的 m 次方, 而 a^m 这种形式的数称为 a 的幂.

求一个数的幂这个过程称为指数化 (数 m 就称为指数). 关于指数化的最基本的事实就是下面的恒等式:

$$a^{m+n}=a^m\cdot a^n,$$

它指出指数化 "把加法化为乘法". 如果看一看下面的小例子, 并且暂时回到老的比较冗长的记号, 就容易看出为什么这个恒等式为真. 例如

$$\begin{aligned}2^7&=2\times2\times2\times2\times2\times2\times2\\&=(2\times2\times2)\times(2\times2\times2\times2)\\&=2^3\times2^4.\end{aligned}$$

假如现在要求我们计算 $2^{3/2}$. 初一看, 这个问题是想岔了路: 上面给出的 2^m 的定义的一个本质的部分, 就是 m 是一个正整数. 把 "一个半"2 乘到一起是没有意义的. 然而数学家喜欢推广, 甚至当我们除了 m 是一个正整数时还不知道 2^m 有什么意思的时候, 也不能阻碍数学家们对于更广泛的数 m 也给 2^m 赋予一种意义.

把推广搞得越是自然, 这种推广就越可能有趣、有意义. 我们使这个推广更加自然的办法, 就是不惜一切代价保持 "把加法化为乘法" 这个性质. 以后会看到, 正是这一点使得对于 $2^{3/2}$ 应该取什么值只有一种明智的选择. 如果这个基本的性质要成立, 就必须令

$$2^{3/2}\cdot2^{3/2}=2^{3/2+3/2}=2^3=8.$$

所以 $2^{3/2}=\pm\sqrt{8}$. 但是取 $2^{3/2}$ 为正数比较方便, 所以定义 $2^{3/2}=\sqrt{8}$.

类似的论据说明 2^0 应该定义为 1. 如果我们想要保持基本性质, 那就应该有

$$2=2^1=2^{1+0}=2^1\cdot2^0=2\cdot2^0.$$

双方除以 2 就有 $2^0=1$.

在这一类论证中我们所做的事是解一个函数方程式, 即一个包含未知函数的方程式. 现在把 2^t 写成 $f(t)$, 这样我们能够看得更加明白. 给出的信息就是这个函数的基本的性质 $f(t+u)=f(t)f(u)$, 再加上这个函数在一点的值: $f(1)=2$. 我们就从这里开始, 并且试图推导出关于 f 的尽可能多的性质.

有一个好习题, 就是证明这两个加于 f 上的条件, 至少是在假设 f 取正值的条件下, 就能决定 f 在每一个有理点的值. 例如对于上面讲过的两个性质, 为了证明 $f(0)$ 应该是 1, 我们注意到 $f(0)f(1)=f(1)$. 至于 $f(3/2)=\sqrt{8}$, 我们已经证明过了, [那时, 我们使用的其实就是作为函数的基本性质的函数方程式]. 证明其他性质

在本质上是类似的, 而结论是 $f(p/q)$ 必须是 2^p 的 q 次根. 更一般地说, $a^{p/q}$ 唯一的明智的定义就是 a^p 的 q 次根.

我们已经从这个基本的函数方程式挖掘出了所有能够挖出的东西, 但是只当 t 为有理数时使得 a^t 有了意义. 当 t 是无理数时, 能不能也对 a^t 赋予明智的定义呢? 例如 $2^{\sqrt{2}}$ 最自然的定义是什么? 因为单纯依靠函数方程式是不能决定 $2^{\sqrt{2}}$ 之值的, 要回答这样的问题就要寻找 f 可能具有的自然的附加性质, 使它和函数方程式一起就能唯一地决定 f. 结果是有两个条件, 它们在一起就能起所需的作用①. 第一个条件是 f 应该是一个**上升函数**, 即是说, 若 $s<t$, 则 $f(s)<f(t)$. 此外还要假设 f 是连续的[I.3 §5.2].

现在看第一个条件在确定 $2^{\sqrt{2}}$ 上怎样起作用. 这里的思想是不去直接计算 $2^{\sqrt{2}}$, 而是去求出它的越来越好的**估计**. 例如, 因为 $1.4<\sqrt{2}<1.5$, 由上述的次序关系 (单调性就是次序关系) 知道 $2^{\sqrt{2}}$ 必在 $2^{7/5}$ 和 $2^{3/2}$ 之间, 而一般地, 只要 $p/q<\sqrt{2}<r/s$, 则 $2^{\sqrt{2}}$ 必在 $2^{p/q}$ 和 $2^{r/s}$ 之间. 可以证明, 当两个有理数 p/q 和 r/s 非常接近时, $2^{p/q}$ 和 $2^{r/s}$ 也非常接近, 所以只要选取这两个有理数越来越接近, 就知道 $2^{p/q}$ 和 $2^{r/s}$ 趋向相同的极限. 由于我们要求 f 是连续的, 所以只能取这个极限为 $2^{\sqrt{2}}$.

2. 指数函数

在数学里, 一个概念真正重要的标志之一是它可以用许多不同的等价的方法来定义, 指数函数 $\exp(x)$ 肯定具有这个特点. 思考它的最基本的方法, 虽然在许多地方不一定是最好的方法, 是把它看成某个数 e 的幂, 即 $\exp(x)=\mathrm{e}^x$. e 的十进小数展开的前一部份是: $2.7182818\cdots$. 为什么我们特别注意这个数? 使得这个数与众不同之处在于如果微分这个函数 $\exp(x)=\mathrm{e}^x$, 仍然会得到 e^x 本身 —— 而且 e 是唯一的具有这个性质的数. 事实上, 这又把我们引导到定义指数函数的第二个方法: 它是微分方程 $f'(x)=f(x)$ 的满足初始条件 $f(0)=1$ 的唯一解.

定义 $\exp(x)$ 的第三个方法, 而且是多数教科书采用的方法是把它定义为幂级数

$$\exp(x)=1+x+\frac{x^2}{2!}+\frac{x^3}{3!}+\cdots$$

之和. 这个级数就是 $\exp(x)$ 的泰勒级数. 上式右方确实是某个数的 x 次幂, 并不是马上就明显可见的, 所以才把它写成 $\exp(x)$, [而不直接写成一个数 a 的幂 a^x, 并且证明 a 就是上述的 e]. 然而, 稍微用一点力气就会看到, 这个级数具有前面讲过的指数函数的那些基本的性质: $\exp(x+y)=\exp(x)\exp(y)$, $\exp(0)=1$ 以及 $(\mathrm{d}/\mathrm{d}x)\exp(x)=\exp(x)$.

① 请特别注意 "在一起" 三个字, 原书似乎可以理解为以下两个条件有一即可. 实际上数学分析的基本常识, 是 "单调性" 和 "连续性" 缺一不可. 实际上原书正文也是这样写的, 所以我在翻译时, 只作了小的改动, 避免误会. —— 中译本注

还有一个定义指数函数的方法, 而这一个更接近于告诉我们指数函数真正的含义究竟是什么. 假如想投资一笔钱十年, 而且有两种选择, 或者十年末的回报是增值 100%(就是翻了一番), 或者在每年末得到回报是当年初您的所有再加上 10%. 您愿取哪一种?

第二种是较好的投资, 因为这时利息是复利, 例如, 如果开始的投资是 \$100, 则一年以后所得是 \$110, 而两年后是 \$121. 第二年增加的 \$11 要分成两部分, 即原有的本金 \$100 在第二年的利息, 以及第一年的利息又有 10%的利息, 即 \$1. 在第二种计算的格式下, 最后所得是 \$100 乘上 $(1.1)^{10}$, 因为每年都要乘 1.1. $(1.1)^{10}$ 的近似值是 2.5937, 所以最后所得几乎是 \$260 而不是 \$200.

如果按月计算复利又如何? 现在就不再是用 $1\dfrac{1}{10}$ 去乘原来的投资十次, 而应该用 $1\dfrac{1}{120}$ 去乘 120 次. 到 10 年结尾, 本金 \$100 会被乘上 $\left(1+\dfrac{1}{120}\right)^{120}$, 它的近似值是 2.707 . 如果按日计算复利, 会把这个倍数增加到接近 2.718 , 这很可疑地接近 e . 事实上, e 可以定义为数 $\left(1+\dfrac{1}{n}\right)^{n}$ 当 $n\to\infty$ 时的极限.

$\left(1+\dfrac{1}{n}\right)^{n}$ 这个式子确有极限这一点不是马上就很明显的. 如果把 m 取为固定的正整数, 则当 $n\to\infty$ 时, $\left(1+\dfrac{1}{n}\right)^{m}\to 1$; 而若固定 n, 则当 $m\to\infty$ 时, $\left(1+\dfrac{1}{n}\right)^{m}\to\infty$. 如果让 $m=n$ 而来看 $\left(1+\dfrac{1}{n}\right)^{n}$, 则幂的增加将和 $1+\dfrac{1}{n}$ 的减小相抵消, 而会得到一个在 2 和 3 之间的极限. 如果 x 是任意实数, 则 $\left(1+\dfrac{x}{n}\right)^{n}$ 也收敛于一个极限, 就定义这个极限为 $\exp(x)$.

下面简略地说一下, 如果这样来定义 $\exp(x)$, 可以得出那些使得这是一个好定义所必须的主要性质, 即 $\exp(x+y)=\exp(x)\exp(y)$. 取

$$\left(1+\frac{x}{n}\right)^{n}\left(1+\frac{y}{n}\right)^{n},$$

它等于

$$\left(1+\frac{x}{n}+\frac{y}{n}+\frac{xy}{n^2}\right)^{n}.$$

现在 $1+x/n+y/n+xy/n^2$ 与 $1+\dfrac{x}{n}+\dfrac{y}{n}$之比小于 $1+xy/n^2$, 而可以证明 $(1+xy/n^2)^n$ 收敛于 1(因为现在幂的增加不足以补偿 xy/n^2 的过快下降). 所以, 当 n 趋于 ∞ 时, $\left(1+\dfrac{x}{n}+\dfrac{y}{n}+\dfrac{xy}{n^2}\right)^{n}$ 与 $\left(1+\dfrac{x+y}{n}\right)^{n}$ 有相同的极限, 而结果得证.

3. 把定义推广到复数

如果将 $\exp(x)$ 看成幂 e^x, 则把定义推广到复数似乎是没有希望的, 我们的直观什么也没有告诉我们, 函数方程没有用, 也不能用连续性和次序关系来决定它.

然而, 幂级数和复利定义都很容易推广到复数情况. 如果 z 是一个复数, 则 $\exp(z)$ 最常用的定义就是

$$1+z+\frac{z^2}{2!}+\cdots.$$

令 $z=\mathrm{i}\theta$, 其中 θ 是实数, 把上面的表达式分开实部和虚部, 就得到

$$1-\frac{\theta^2}{2!}+\frac{\theta^4}{4!}+\cdots+\mathrm{i}\left(\theta-\frac{\theta^3}{3!}+\frac{\theta^5}{5!}-\cdots\right).$$

利用 $\cos\theta$ 和 $\sin\theta$ 的幂级数展开式, 就有 $\exp(\mathrm{i}\theta)=\cos\theta+\mathrm{i}\sin\theta$, 这就是复平面上的单位圆周上的幅角为 θ 的点. 特别是若取 $\theta=\pi$, 就会得到著名的公式 $\mathrm{e}^{\mathrm{i}\pi}=-1$(因为 $\cos\pi=-1$ 而 $\sin\pi=0$).

这个公式如此惊人, 所以人们觉得它应该有一个好的理由, 而不只是进行了一些形式的代数运算后偶然碰上的一个结果. 为了看出这个理由, 我们回到复利的思想, 并定义 $\exp(z)$ 为当 $n\to\infty$ 时 $\left(1+\dfrac{z}{n}\right)^n$ 的极限. 我们专注于 $z=\mathrm{i}\pi$ 的情况, 为什么当 n 很大时, $(1+\mathrm{i}\pi/n)^n$ 会接近于 -1 呢?

要回答这个问题, 我们从几何上来看. 一个复数乘以 $1+\mathrm{i}\pi/n$ 的几何效果是什么呢? 在阿尔干图形上这个复数是很接近于 1, 而且位于 1 的垂直上方. 因为过 1 的铅直线必定是单位圆周在 $z=1$ 处的切线, 所以 $1+\mathrm{i}\pi/n$ 这个数必定是很近于单位圆周上幅角为 π/n 的那个数 (因为单位圆周上的一个数的幅角就是从 1 开始计算的圆弧的长度, 而在我们的情况, 因为 n 很大, 所以圆弧几乎就是直线). 所以, 一个复数乘以 $1+\mathrm{i}\pi/n$ 非常近于旋转一个角度 π/n. 这样作了 n 次就是旋转一个角度 π, 也就是乘以 -1 . 用类似的论据可以看到 $\exp(\mathrm{i}\theta)=\cos\theta+\mathrm{i}\sin\theta$ 的理由.

下面按照这样的思路来理解为什么指数函数的导数仍是指数函数. 已知 $\exp(z+w)=\exp(z)\exp(w)$, 所以 $\exp(z)$ 在 z 点的导数就是 $\exp(z)\left(\exp(w)-1\right)/w$ 当 w 趋于 0 时的极限. 所以只要证明当 w 很小时 $\exp(w)-1$ 非常接近于 1 就够了. 为要对于 $\exp(w)$ 有一个好的感觉, 只需要取一个很大的 n, 再看 $(1+w/n)^n$ 就行了. 证明它的极限是 $1+w$ 本来不难, 但是我们宁可用一个非形式的论证. 假设您的银行账户只给您很小的年利率, 比方说是 0.5%. 如果把它改成按月取复利, 可以得到多大的好处? 答案是: 好处不大. 如果利息的总量已经很小, 那么, 利息的利息更是可以忽略不计. 从本质上说, 这就是 $(1+w/n)^n$ 可以用 $1+w$ 来逼近的理由.

我们还可以把指数函数的定义进一步推广. 指数函数的主要成分就是加法、乘法, 以及允许取极限. 所以, 举例来说, 如果 x 是一个巴拿赫代数[III.12]A 的元素, $\exp(x)$ 就是有意义的 (在这里, 幂级数定义是最容易的, 但是不一定是最有启发的).

4. 对数函数

自然对数和指数函数一样有多种定义的方法. 下面是其中三种:

(i) 函数 log 是函数 exp 的反函数. 就是说, 如果 t 是一个正实数, 则命题 $u=\log(t)$ 等价于命题 $t=\exp(u)$.

(ii) 令 t 为一正实数, 则

$$\log(t)=\int_1^t \frac{dx}{x}.$$

(iii) 若 $|x|<1$, 则 $\log(1+x)=x-\frac{x^2}{2}+\frac{x^3}{3}-\cdots$. 此式在 $0<t<2$ 上定义了 $\log(t)$. 若 $t\geqslant 2$, 则 $\log(t)$ 可以定义为 $-\log(1/t)$.

对数函数最重要的特性仍然是一个函数方程式, 恰好就是把指数函数的函数方程式反过来, 即是 $\log(st)=\log(s)+\log(t)$. 所以 exp 变加法为乘法, 而 log 变乘法为加法. 这个事实的一个比较形式的说法是: $\mathbf{R}$ 在加法下成群, 而正实数的集合 $\mathbf{R}_+$ 在乘法下成群. 函数 exp 是从 $\mathbf{R}$ 到 $\mathbf{R}_+$ 的同构, 而它的反函数 log 则是从 $\mathbf{R}_+$ 到 $\mathbf{R}$ 的同构. 所以在一定意义下, 这两个群有相同的结构, 而指数和对数函数就证明了这一点.

现在让我们用 log 的第一种定义来看为什么 $\log(st)$ 必须等于 $\log(s)+\log(t)$. 写出 $s=\exp(a)$, $t=\exp(b)$. 则 $\log(s)=a$, $\log(t)=b$. 而

$$\begin{aligned}\log(st)&=\log(\exp(a)\cdot\exp(b))\\&=\log(\exp(a+b))\\&=a+b.\end{aligned}$$

结果得证.

一般来说 log 的性质是紧紧追随着 exp 的性质的, 然而有一个非常重要的区别来自企图把 log 推广到复数所引起的复杂性. 一开始是很简单的, 每一个复数 z 都可以利用一个非负的实数 r 和某个 θ 写成 $r\mathrm{e}^{\mathrm{i}\theta}$($r$ 和 θ 分别是 z 的模和幅角). 如果 $z=r\mathrm{e}^{\mathrm{i}\theta}$, 则我们会想到 $\log(z)$ 应该是 $\log(r)+\mathrm{i}\theta$(这里利用了 log 的函数方程式, 以及 log 和 exp 互为反函数). 这里的问题是 θ 并非唯一决定的. 例如 $\log(1)=?$ 正常情况下, 我们会说它等于 0, 但是也可以偏偏要说, 因为 $1=\mathrm{e}^{2\pi\mathrm{i}}$, 所以 $\log(1)=2\pi\mathrm{i}$.

因为有这样的困难, 找不到一个最好的方法在整个复数平面上定义对数函数, 哪怕把 0, 一个不论怎么看都没有对数的数, 从复数平面上挖掉也不行. 有一个规定是在非零的 $z=r\mathrm{e}^{\mathrm{i}\theta}$ 中令 $r>0$, $0\leqslant\theta<2\pi$, 这样 z 就只有一种写法, 然后定义 $\log(z)=\log(r)+\mathrm{i}\theta$. 但是这样一来 log 这个函数就是不连续的了, 如果从 [上半平面] 越过正实轴跳 [到下半平面], 则幅角有了一个跳跃 2π, 而对数也就有了一个跳跃 $2\pi\mathrm{i}$.

值得注意的是, 这不但不是对与数学的一个打击, 而是一个完全具有正面意义的事, 它正是复分析的好几个重要定理背后的实质, 例如柯西的留数定理, 这个定理使我们能够计算很一般的路径积分.

III.26　快速傅里叶变换 (The Fast Fourier Transform)

如果 $f:\mathbf{R}\to\mathbf{R}$ 是一个周期为 1 的周期函数, 通过计算它的傅里叶系数就可以获得大量有关 f 的信息 (见傅里叶变换[III.27], 其中讨论了其原因何在). 这一点在理论上和实践上都是如此, 而由于实践上的理由, 非常希望有一种好的方法来快速地计算傅里叶系数.

第 r 个傅里叶系数是由以下公式给出的:

$$\hat{f}(r)=\int_0^1 f(x)\,\mathrm{e}^{-2\pi\mathrm{i}rx}\mathrm{d}x.$$

如果没有 f 的显式的公式来计算上面的积分 (例如当 f 是由物理讯号给出, 而不是由数学公式给出时, 就是这样), 就需要从数值上来逼近这个积分, 而做这件事的自然的方法是把它**离散化**, 就是把积分换成以下形式的和: $N^{-1}\sum_{n=0}^{N-1}f(n/N)\times\mathrm{e}^{-2\pi\mathrm{i}rn/N}$. 如果 f 不是震荡得太剧烈, r 又不太大, 这将是一个好的逼近.

如果对上式中的 r 加上 N 的整数倍, 这个积分和的值不会改变, 所以只需考虑 $\hat{f}$ 在形如 n/N (n 为一切整数) 的点处的值①. 同样, 因为 f 以 1 为周期, 所以若对 n 加上 N 的整数倍也不会影响上式. [既然对 r 和 N 都允许加上 N 的整数倍], 所以可以认为 r 和 N 都是群 $\mathbf{Z}_N$(整数 mod N 所成的群见模算术[III.58]). 现在把记号稍作改动来反映这件事: 给定了一个定义在 $\mathbf{Z}_N$ 上的函数 g, 定义同样是定义在 $\mathbf{Z}_N$ 上的函数

$$\hat{g}(r)=N^{-1}\sum_{n\in\mathbf{Z}_N}g(n)\,\omega^{-rn}\tag{1}$$

为 g 的离散傅里叶变换 (以下简记为 DFT), 其中用 ω 来代表 $\mathrm{e}^{2\pi\mathrm{i}/N}$, 所以 $\omega^{-rn}=\mathrm{e}^{-2\pi\mathrm{i}rn/N}$, 注意这里的求和就是对 n 从 0 到 $N-1$ 求和, 和前面一样. 再有一个记号变化就是用 $g(n)$ 代替了 $f(n/N)$.

DFT 可以看成是用一个 $N\times N$ 矩阵 (其元素为 ω^{-rn} , r , $n\in\mathbf{Z}_N$) 去乘一个列向量 (其元素为 $g(n)$, $n\in\mathbf{Z}_N$). 所以这里需要 N^2 个算术运算. 快速傅里叶变换 (以下简记为 FFT) 的出现则是由于看到了 (1) 中的和具有的对称性质, 使得其计算可以大为更加有效地进行. 当 N 为 2 的幂时, 这一点最容易看见, 而为了做得更加容易一些, 令 $N=8$, 想要求的和是

$$g(0)+\omega^{-r}g(1)+\omega^{-2}g(2)+\cdots+\omega^{-7}g(7),$$

①原书这里误将 $\hat{f}$ 写成 f, 这样就和下面限制 f 只在 n/N 处取值相重复, 故译文作了修改. —— 中译本注

其中的 r 也取从 0 到 7 的某个整数值. 这样一个和可以重写为

$$g(0)+\omega^{-2r}g(2)+\omega^{-4r}g(4)+\omega^{-6r}g(6)$$
$$+\omega^{-r}g(1)+\omega^{-3r}g(3)+\omega^{-5r}g(5)+\omega^{-7r}g(7),$$

有趣的是

$$g(0)+\omega^{-2r}g(2)+\omega^{-4r}g(4)+\omega^{-6r}g(6)$$

和

$$g(1)+\omega^{-2r}g(3)+\omega^{-4r}g(5)+\omega^{-6r}g(7)$$

都是某个函数的 DFT. 例如, 设 $h(n)=g(2n)$, $0\leqslant n\leqslant 3$, 并记 $\psi=\omega^2=\mathrm{e}^{2\pi\mathrm{i}/4}$, 则上面第一个式子现在就成了 $h(0)+\psi^{-r}h(2)+\psi^{-2r}h(2)+\psi^{-3r}h(3)$. 如果我们认为 h 是定义在 $\mathbf{Z}_4$ 上的, 这恰好就是 $\hat{h}(r)$ 的公式.

对于第二个表达式, 也可以作类似说明, 所以, 如果对 g 的 "偶部" 和 "奇部" 作 DFT, 就很容易直接得到 g 本身的傅里叶变换的每一个值, 这个值只不过是偶部和奇部的傅里叶变换值的线性组合而已. 这样, 若 N 是偶数, 用 $F(N)$ 来表示计算定义在 $\mathbf{Z}_N$ 上的函数的 DFT 所需要的算术运算的次数, 就会得到以下叙述的递推公式:

$$F(N)=2F(N/2)+CN\ .$$

这个公式的意思就是: 如果要算出定义在 $\mathbf{Z}_N$ 上的某个函数的傅里叶变换的 N 个值, 只需作两次定义在 $\mathbf{Z}_{N/2}$ 上的函数的傅里叶变换的 $N/2$ 个值, 再加上 N 个线性组合, 每一个需要一个常数步数.

如果 N 是 2 的幂, 就可以用迭代方法进行如下: $F(N/2)$ 是 $2F(N/4)+CN/2$ (但这里的 C 与上面的可以不同). 并仿此以往, 不难证明, 最后的结果是 $F(N)\leqslant CN\log N$, 其中 C 是某个常数, 比之 CN^2 这当然是很大的改进. 如果 N 不是 2 的幂, 上面的论证当然不行了. 但是对这个方法可以作某些修正, 并得到类似的效率的收益 (事实上, 对于任意有限阿贝尔群上的傅里叶变换, 这都是对的).

一旦我们会有效地计算傅里叶变换了, 有许多其他计算也同样变得容易了. **逆傅里叶变换**是一个简单的例子, 因为它有一个类似的公式使它也可以类似地来计算. 再一个例子是两个序列的**卷积**, 其定义如下: 若 $a=(a_0,a_1,a_2,\cdots,a_m)$, $b=(b_0,b_1,b_2,\cdots,b_n)$ 是两个序列, 它们的卷积就是序列 $c=(c_0,c_1,c_2,\cdots,c_{m+n})$, 其中的 c_r 定义为 $a_0b_r+a_1b_{r-1}+\cdots+a_rb_0$, 序列 c 记作 $a*b$. 傅里叶变换的最重要的性质之一就是 "变卷积为乘积". 就是说, 如果有了一个适当的方法把 a 和 b 都看作 $\mathbf{Z}_N$ 上的函数, 则 $a*b$ 的傅里叶变换就是一个函数 $r\mapsto\hat{a}(r)\hat{b}(r)$. 所以想要做出 $a*b$, 只需作出 $\hat{a}$ 和 $\hat{b}$, 把它们乘起来, 再作其积的逆傅里叶变换. 计算的每一个阶段都很快, 所以整个计算也很快.

这导出一种求两个多项式 $a_0 + a_1x + \cdots + a_mx^m$ 和 $b_0 + b_1x + \cdots + b_nx^n$ 的乘积的快速的方法, 因为它们的乘积的系数正是由系列 $c = a * b$ 给出的. 如果所有的 a_i 都在 0 到 9 之间, 就有了一个计算两个多项式在 $x = 10$ 处之值的快速的方法 (因为每一个系数 c_r 的位数都不高), 所以也就有了一个计算两个 n 位数的比长乘法更快的方法. 这样, 就有了快速傅里叶变换的为数巨大的应用中的两个. 工程是一个更直接的应用的来源, 因为在工程里, 我们时常想通过研究信号的傅里叶变换来分析这些信号. 它对于量子计算[III.74] 的应用是非常惊人的, Peter Shor 有一个著名的结果, 就是可以用量子计算机来非常快地对大数作因数分解, 这个算法很本质地依赖于快速傅里叶变换, 但是又奇迹般地应用量子计算机的能力, 把 $N \log N$ 步分成 N 批, 每批 $\log N$ 步, 而这 N 批可以 "并行计算".

III.27 傅里叶变换

(The Fourier Transform)

陶哲轩 (Terence Tao)

令 f 为一个由 $\mathbf{R}$ 到 $\mathbf{R}$ 的函数. 在典型情况下对于 f 并没有什么可说的, 但是有些函数具有有用的对称性质. 例如, 若对于每一个 x 都有 $f(-x) = f(x)$, 就说 f 是一个**偶函数**, 而若对每一个 x 有 $f(-x) = -f(x)$, 就说 f 是一个**奇函数**. 进一步说, 每一个函数 f 都可以写成一个偶函数 f_{e}(称为 f 的偶部) 和一个奇函数 f_{o}(称为 f 的奇部) 的**叠加**. 例如, 函数 $f(x) = x^3 + 3x^2 + 3x + 1$ 既不是偶的, 也不是奇的, 但是, 它可以写成 $f_{\mathrm{e}}(x) + f_{\mathrm{o}}(x)$, 其中 $f_{\mathrm{e}}(x) = 3x^2 + 1$, $f_{\mathrm{o}}(x) = x^3 + 3x$. 对于一般的函数 f, 这种分解是唯一的, 而由公式

$$f_{\mathrm{e}}(x) = \frac{1}{2}(f(x) + f(-x))$$

和

$$f_{\mathrm{o}}(x) = \frac{1}{2}(f(x) - f(-x))$$

给出.

偶函数和奇函数有什么样的对称性呢? 下面是一个对待它们的有用的方法. 有一个由实数轴上的两个变换构成的群: 一个变换是恒等变换 $\iota: x \mapsto x$, 另一个是反射 $\rho: x \mapsto -x$. 实轴上的任意变换 ϕ 都会诱导出定义在实轴上的函数的变换如下: 给定一个定义在实轴上的函数 f, 变换后的函数就是 $g(x) = f(\phi(x))$. 对于当前的情况, 若 $\phi = \iota$, 则变换后的函数是就是 $f(x)$ 本身, 而若 $\phi = \rho$, 则得到 $f(-x)$. 若 f 是偶函数或奇函数, 则变换后的函数是原来函数 f 的**标量倍数**. 特别是若 $\phi = \rho$,

则当 f 为偶函数时, 变换后的函数仍为 $f(x)$, 而作为倍数的标量是 1; 当 f 为奇函数时, 则变换后的函数是 $-f(x)$ 而这个标量是 -1.

上面描述的过程可以看作是傅里叶变换的一般概念的很简单的原型. 非常广泛地讲, 一个傅里叶变换就是一种把非常 "一般" 的函数分解为 "对称" 函数的叠加的系统方法. 这些对称的函数通常都是显式定义的, 例如, 最重要的就是分解为三角函数[III.92]$\sin(nx)$ 和 $\cos(nx)$ 的线性组合, 它们也时常与频率和能量这些物理概念相关. 对称性一般是与一个群[I.3 §2.1]G 相联系的, 这个群又通常是阿贝尔群 (在上面的例子中, 它是一个含两个元素的群). 说真的, 傅里叶变换是研究群的理论, 准确一些说是研究群表示理论[IV.9] 的基本工具, 这个理论关注的就是一个群可以怎样在不同方式下看成是对称群. 傅里叶变换也与线性代数的一些主题有关, 例如, 向量之表示为规范正交基底[III.37] 的线性组合, 或者表示为一个矩阵或线性算子[III.50] 的本征向量[I.3 §4.3] 的线性组合.

现在来看一个比较复杂的例子. 固定一个正整数 n, 我们要给出一个把由 $\mathbf{C}$ 到 $\mathbf{C}$ 的函数, 即复平面上的复函数加以分解的系统方法. 若 f 是这样一个函数, 而 j 是介于 0 到 $n-1$ 间的整数, 我们说 f 是一个 j 阶**谐振子**, 如果它有以下的性质: 令 $\omega=\mathrm{e}^{2\pi\mathrm{i}/n}$, 即若 ω 是 1 的一个 n 阶本原单位根 (即有 $\omega^n=1$, 但 ω 的次数较小的幂不会给出 1), 这时, 对于任意的复数 $z\in\mathbf{C}$, 有 $f(\omega z)=\omega^j f(z)$. 注意, 若 $n=2$, 则 $\omega=-1$, 所以若 $j=0$ 就会回到偶函数的定义, 而若 $j=1$, 就回到奇函数的定义. 事实上, 受到这件事的启发, 就会得到把 f 分解为谐振子的一般公式, 而这种展开也是唯一的. [其作法如下]: 若定义

$$f_j(z)=\frac{1}{n}\sum_{k=0}^{n-1} f\left(\omega^k z\right)\omega^{-jk},$$

则证明对于任意复数 $z\in\mathbf{C}$ 有

$$f(z)=\sum_{j=0}^{n-1} f_j(z)$$

只是一个简单的习题 (证明中要用到, 当 $k=0$ 时, $\sum_j \omega^{-jk}=n$, 而对于 $k\neq 0$, 此式为 0), 而且还有 $f_j(\omega z)=\omega^j f_j(z)$. 这样, f 可以分解为谐振子之和. [这就是一个傅里叶变换], 而与它相联系的群就是 n 阶单位原根 $1, \omega, \cdots, \omega^{n-1}$ 的乘法群, 即 n 阶循环群. 根 ω^j 表示复平面上旋转一个角 $2\pi j/n$.

现在考虑无限群. 令 f 为定义在单位圆周 $T=\{z\in\mathbf{C}:|z=1|\}$ 上的一个复函数. 为了避免一些技术上的问题, 假设 f 为光滑的, 即无限可微的. 如果 f 是一个形状简单的函数 cz^n, n 是一个整数 [(可以是 0 或负的)], 而 c 是一个常数, 则 f 有 n 阶的旋转对称性. 即是说, 若再令 $\omega=\mathrm{e}^{2\pi\mathrm{i}/n}$, 则对于任意复数 $z\in\mathbf{C}$,

$f(\omega z) = f(z)$. 从前面的例子看到, 并不惊奇, 任意光滑函数 f 都可以表示为这种旋转对称函数的叠加. 事实上, 有

$$f(z) = \sum_{n=-\infty}^{\infty} \hat{f}(n) z^n,$$

数 $\hat{f}(n)$ 称为 f 在频率为 n 处的傅里叶系数, 而由下式给出:

$$\hat{f}(n) = \frac{1}{2\pi} \int_0^{2\pi} f\left(e^{i\theta}\right) e^{-in\theta} d\theta .$$

这个公式可以看作是上面 $f_j(z)$ 的公式当 z 限制在单位圆周上且 $n \to \infty$ 时的极限. 它也可以看作是全纯函数[I.3 §5.6] 的泰勒级数的推广: 若 f 在闭单位圆盘 $\{z \in \mathbf{C} : |z| \leqslant 1\}$ 上是全纯的, 则有

$$f(x) = \sum_{n=0}^{\infty} a_n z^n,$$

而泰勒系数 a_n 由下式给出

$$a_n = \frac{1}{2\pi i} \int_{|z|=1} f(z)\, dz / z^{n+1}$$

一般说来, 傅里叶分析与复分析有很紧密的联系.

如果 f 是光滑的, 则其傅里叶系数衰减于 0 非常快, 而很容易证明其傅里叶级数 $\sum_{n=-\infty}^{\infty} \hat{f}(n) z^n$ 收敛. 但是, 如果 f 不是光滑的 (例如只是连续的), 问题就微妙多了, 这时必须仔细确定这个级数收敛的确切的意义. 实际上调和分析[IV.11] 的相当一部分就是在讨论这一类问题, 以及解决这类问题所需的工具.

与傅里叶分析的这种讲法相关的群是圆周的群 $\mathbf{T}$(注意, 我们既把数 $e^{i\theta}$ 看成圆周上的一点, 又把它看成旋转一个角 θ. 这样, 这个圆周和它的旋转对称群可以等同起来, [所以上面说到圆周的群 T]. 但是还有第二个群在这里也很重要, 即所有整数所成的加法群 $\mathbf{Z}$. 如果取两个基本的对称函数 z^m 和 z^n 并把它们乘起来, 就会得到 z^{m+n}, 所以映射 $n \mapsto z^n$ 就是由 $\mathbf{Z}$ 到这些函数在乘法下所成的群的同构. 群 $\mathbf{Z}$ 就称为 T 的**庞特里亚金对偶**.

在偏微分方程以及调和分析的相关领域里, 最重要的傅里叶变换是定义在欧几里得空间 $\mathbf{R}^d$ 上的. 在所有的函数 $f : \mathbf{R}^d \to \mathbf{C}$ 中, 取**平面波** $f(x) = c_\xi e^{2\pi i x \cdot \xi}$ 为"基本的" 函数, 这里 $\xi \in \mathbf{R}^d$ 是一个向量 (称为平面波的**频率**), $x \cdot \xi$ 是位置向量 x

和频率向量 ξ 的数量积, 而 c_ξ 是一个复数 (其大小称为平面波的**振幅**). 注意, 形如 $H_\lambda=\{x:x\cdot\xi=\lambda\}$ 是正交于向量 ξ 的 (超) 平面, 在每一个这样的集合上, 平面波 $f(x)$ 取常数值, 而 f 在 H_λ 上的值与在 $H_{\lambda+2\pi}$ 上的值相同. 平面波一词即由此而来. 可以证明, 若 f 相当 "好"(例如是光滑的, 而且当 x 变大时衰减到 0 相当快), 它就可以唯一地表示为平面波的叠加, 不过这里的 "叠加" 要用一个积分而不是求和来表示. 更确切地说, 有①

$$f(x)=\int_{\mathbf{R}^d}\hat{f}(\xi)\,\mathrm{e}^{2\pi\mathrm{i}x\cdot\xi}\mathrm{d}\xi\,,$$

其中

$$\hat{f}(\xi)=\int_{\mathbf{R}^d}f(x)\,\mathrm{e}^{-2\pi\mathrm{i}x\cdot\xi}\mathrm{d}x\,.$$

函数 $\hat{f}(\xi)$ 就称为 f 的**傅里叶变换**, 而前一个公式则称为**逆傅里叶变换公式**. 这两个公式告诉我们怎样从原来的函数求出其傅里叶变换, 以及相反. 我们可以把量 $\hat{f}(\xi)$ 看成是 f 中所包含的按频率 ξ 震荡的成分有多少. 可以证明, 当 f 相当 "好" 的时候, 论证这些积分的收敛性毫无困难, 然而当 f 比较粗糙或者衰减得不太快的时候, 这些问题又变得很微妙. 在 $\mathbf{R}^d$ 上的傅里叶变换的情况下, 相关的群是欧几里得群 $\mathbf{R}^d$(这里也是把 $\mathbf{R}^d$ 既看成欧几里得空间, 又看作这个空间的平移群). 还要注意, 现在位置 x 和频率 ξ 都含于 $\mathbf{R}^d$ 内, 所以 $\mathbf{R}^d$ 在这个背景下, 正是自己的庞特里亚金对偶②.

傅里叶变换的一大用途是用它来理解作用在函数上的各种算子, 例如, $\mathbf{R}^d$ 上的拉普拉斯算子. 给定一个函数 $f:\mathbf{R}^d\to\mathbf{C}$, 拉普拉斯算子 Δf 的定义是

$$\Delta f(x)=\sum_{j=1}^{d}\frac{\partial^2 f}{\partial x_j^2}\,,$$

这里把向量 x 写成分量形式, 而把 f 看成 d 个实变量的函数 $f(x_1,\cdots,x_d)$. 为了避免技术细节, 只考虑那些足够光滑使得上式有意义而不产生困难的情况. 一般说

① 在有些教本上, 傅里叶变换的定义稍有不同, 例如, 上面两个式子分别写成

$$f(x)=(2\pi)^{-d}\int_{\mathbf{R}^d}\hat{f}(\xi)\,\mathrm{e}^{\mathrm{i}x\cdot\xi}\mathrm{d}\xi \text{ 和 } \hat{f}(\xi)=\int_{\mathrm{R}^d}f(x)\,\mathrm{e}^{-\mathrm{i}x\cdot\xi}\mathrm{d}x\,.$$

这种记号上的小变动有好处也有毛病, 但它们都是等价的 (译者把原文稍作了变动, 使得对我国读者方便一点). —— 中译本注

②这是因为依赖于我们使用了欧几里得数量积的缘故. 如果改用其他数量级, 则庞特里亚金对偶将是 $(\mathbf{R}^d)^*$, 但是这些细微之处对于绝大多数应用并不重要.

来, 一个函数 f 和它的拉普拉斯算子 Δf 之间并无明显的关系. 但是, 若 f 是平面波 $f(x)=\mathrm{e}^{2\pi ix\cdot\xi}$, 则二者有明显的关系:

$$\Delta \mathrm{e}^{2\pi ix\cdot\xi}=-4\pi^2|\xi|^2\mathrm{e}^{2\pi ix\cdot\xi}.$$

就是说拉普拉斯算子作用在平面波上的效果就是把它乘以标量 $-4\pi^2|\xi|^2$. 换句话说, 平面波是 Δf 关于本征值 $-4\pi^2|\xi|^2$ 的本征函数① (一般说来, 平面波将是任意与平行移动可交换的线性算子的本征函数). 所以, 透过傅里叶变换的棱镜来看拉普拉斯算子是很简单的: 傅里叶变换使我们能把任意的函数写成平面波的叠加, 而拉普拉斯算子在每一个平面波上的效果又很简单. 讲清楚一点, 就是

$$\begin{aligned}\Delta f(x)&=\Delta\int_{\mathbf{R}^d}\hat{f}(\xi)\mathrm{e}^{2\pi ix\cdot\xi}\mathrm{d}\xi=\int_{\mathbf{R}^d}\hat{f}(\xi)\Delta\mathrm{e}^{2\pi ix\cdot\xi}\mathrm{d}\xi\\&=\int_{\mathbf{R}^d}\left(-4\pi^2|\xi|^2\right)\hat{f}(\xi)\mathrm{e}^{2\pi ix\cdot\xi}\mathrm{d}\xi.\end{aligned}$$

此式给出了拉普拉斯算子作用在一般函数上的公式. 在这里交换了拉普拉斯算子 Δ 与积分的次序. 对于适当好的函数, 这是可以严格论证的, 但是我们略去细节.

这个公式把 Δf 表示为平面波的叠加. [此外, 逆傅里叶变换的公式又告诉我们

$$\Delta f(x)=\int_{\mathbf{R}^d}\widehat{\Delta f}(\xi)\mathrm{e}^{2\pi ix\cdot\xi}\mathrm{d}\xi.$$

但是, 一个函数表示为平面波的叠加的方法是唯一的], 所以

$$\widehat{\Delta f}(\xi)=\left(-4\pi^2|\xi|^2\right)\hat{f}(\xi),$$

这一个事实当然也可以由傅里叶变换的定义直接导出. 这个恒等式说明, 傅里叶变换把拉普拉斯算子**对角化**, 就是说, 从傅里叶变换看来, 对某个函数施加拉普拉斯算子, 无非就是把这个函数的傅里叶变换 $F(\xi)$ 乘以**乘子**$-4\pi^2|\xi|^2$. $-4\pi^2|\xi|^2$ 这个量可以解释为与频率 ξ 相关的能级②. 换言之, 拉普拉斯算子可以看成一个傅里叶乘子. 这句话的意思是, 如果想要计算拉普拉斯算子对于一个函数的作用, 可以先取这个函数的傅里叶变换, 乘上乘子, 再取逆傅里叶变换. 这个观点使得拉普拉斯算子的操作变得很容易. 例如, 可以迭次使用这个公式来计算拉普拉斯算子的各次幂:

$$\widehat{\Delta^n f}(\xi)=\left(-4\pi^2|\xi|^2\right)^n\hat{f}(\xi),\quad n=0,1,2,\cdots.$$

事实上, 现在已经可以定义拉普拉斯算子的更加一般的函数. 例如, 可以取拉普拉斯算子的平方根如下:

$$\widehat{\sqrt{-\Delta}f}(\xi)=2\pi|\xi|\hat{f}(\xi).$$

①严格说是一个**广义本征函数**, 因为平面波在 $\mathbf{R}^d$ 上不是平方可积的.

②采用这种能级的观点时, 拉普拉斯算子习惯上写为 $-\Delta$ 而非 Δ, 这样来使得能量为正.

这就会引导到分数阶微分算子理论 (而这又只是**拟微分算子**的特例), 还有更一般的函数演算[IV.15 §3.1](functional calculus) 理论, 在其中, 我们从某一个算子 (如拉普拉斯算子) 开始, 然后研究这个算子的各种函数, 例如平方根、指数、倒数, 等等.

正如上面的讨论所表明的那样, 傅里叶变换可以用来发展许多有趣的运算, 而这对于微分方程理论有特别的重要性. 为了有效地分析这些运算, 需要傅里叶变换的种种**估计**. 例如, 了解一个函数 f 的用某种范数表示的大小, 与其傅立叶变换的可能用其他范数来表示的大小的关系, 这时常是重要的. 关于这一点的进一步讨论可见条目函数空间[III.29]. 这种类型的估计中特别重要而又惊人的是**普兰舍利**(Michel Plancherel , 1885 – 1967, 瑞士数学家)**公式**

$$\int_{\mathbf{R}^d} |f(x)|^2\,\mathrm{d}x = \int_{\mathbf{R}^d} \left|\hat{f}(\xi)\right|^2 \mathrm{d}\xi.$$

它表明, 一个函数的傅里叶变换的 L_2 范数与原来函数的 L_2 范数**恰好相等**. 所以, 傅里叶变换是一个酉变换, 因此可以把一个函数的频率空间表示看成是它的物理空间表示的某种意义的**旋转**.

发展与傅里叶变换以及相关算子的进一步的估计是调和分析的很大一个部分. 普兰舍利恒等式的一个变体的傅里叶变换的卷积公式

$$\int_{\mathbf{R}^d} f(y)\,g(x-y)\,\mathrm{d}y = \int_{\mathbf{R}^d} \hat{f}(\xi)\,\hat{g}(\xi)\,\mathrm{e}^{2\pi i x\cdot\xi}\mathrm{d}\xi.$$

这个公式使我们能用两个函数 f 和 g 的傅里叶变换来分析它们的卷积

$$f * g(x) = \int_{\mathbf{R}^d} f(y)\,g(x-y)\,\mathrm{d}y.$$

特别是, 若 f 或 g 的傅里叶变换[①]很小, 则我们可以期望它们的卷积 $f*g$ 也很小. 这个关系意味着傅里叶变换控制了一个函数和它自己以及和其他函数的某些**相关性**, 这就使得傅里叶变换成了研究随机性以及概率理论、调和分析和数论中的其他对象的均匀分布性质的重要工具. 例如, 我们可以追随这个思想来确立中心极限定理, 这个定理表明许多独立随机变量的和最终会像是一个高斯分布[III.71 §5]; 我们甚至可以用这个方法来证明维诺格拉多夫(Ivan Matveevich Vinogradov , 1891–1983, 前苏联数学家)定理[V.27]: 任意充分大的奇数都是三个素数之和.[②]

以上这些思想可以在多个方向上推广. 例如, 可以用比较一般的算子代替拉普拉斯算子, 用这个算子的 (广义) 本征函数代替平面波, 这样就得到谱的理论[III.86]和函数演算. 也能抽象地研究傅里叶乘子 (或卷积) 的代数, 这就引导到C^*-代数

①原书作傅里叶系数, 但是这里没有讨论系数. —— 中译本注

②最近, 在法国工作的秘鲁数学家 H. Helfgott 已经证明了任意 $\geqslant 7$ 的奇数都可以示成三个系数之和. 详见条目解析数论[IV.2] 的一个脚注. —— 中译本注

[Ⅳ.15 §3] 还可以越出线性算子理论来研究双线性、多线性甚至完全非线性算子, 这特别会引导到**仿积**(paraproduct) 的理论. 仿积是点态乘积运算 $(f(x), g(x)) \mapsto fg(x)$ 的推广, 它在微分方程中有重要性. 在另一个方向上, 也能用更一般的群来代替 $\mathbf{R}^d$, 这时, 平面波的概念就会被**群特征标**概念 (在阿贝尔群的情况) 取代, 或者被群的**表示**(在非阿贝尔群的情况) 所取代. 傅里叶变换还有其他变体, 如拉普拉斯变换、梅林 (Robert Hjalmar Mellin, 1854–1933, 芬兰数学家) 变换 (关于其他的变换, 详见条目变换[III.91]), 它们在代数上很像傅里叶变换, 而且作用也相似 (例如, 拉普拉斯变换在微分方程上所起的作用). 我们已经看到傅里叶变换与泰勒级数有关, 它还与其他重要的级数展开式有联系, 需要提到的有狄利克雷级数, 以及函数按特殊多项式[III.85] 的级数展开, 例如, 按正交多项式或球面调和[III.87] 的展开式.

傅里叶变换是把函数分成许多成分, 而每一个成分恰好有一个准确的频率. 但在有些应用中, 采取一种比较 "模糊" 的途径更为有用. 这时, 函数被分解成的成分数目要少一些, 但是每一个成分所含的频率构成一个频段, 而不是单个频率. 这样一种分解有一个优势, 就是受到**不确定性原理**的限制较少. 因为按照不确定性原理, 一个函数及其傅里叶变换不可能同时局限在 $\mathbf{R}^d$ 的很小的区域里. 这样会导致傅里叶变换的某些变体, 如小波变换[Ⅶ.3], 它对许多应用数学和计算数学问题更为适合, 也对某些调和分析和微分方程的问题更为适合. 对于量子力学起基本作用的不确定性原理也把傅里叶变换与数学物理联系起来, 特别是经典物理和量子物理的联系, 可以通过几何量子化和微局部分析的方法作严格的研究.

III.28 富克斯群
(Fuchsian Groups)

Jeremy Gray

几何学的最基本的图形之一是**环面**, 这是一个轮胎形的曲面. 如果想要作一个环面, 可以取一个正方形, 并且先把它的一对对边, 例如, 上下对边粘起来, 这样就得到了一个柱面, 然后再把它的另外一对对边 (即原来正方形的左右对边) 粘起来, 就得到了环面.

下面是环面的更加数学化的作法. 我们从通常的 (x, y) 坐标平面开始, 在其中作以四点 $(0, 0)$, $(1, 0)$, $(1, 1)$, $(0, 1)$ 为顶点的正方形, 它是由坐标适合 $0 \leqslant x \leqslant 1$, $0 \leqslant y \leqslant 1$ 的点构成的. 可以在水平和铅直两个方向上移动这个正方形. 如果在水平方向移动 m 个单位, 在铅直方向上移动 n 个单位, 这里 m 和 n 是整数, 就会得到由坐标适合下面的不等式的点所成的正方形: $m \leqslant x \leqslant m+1$, $n \leqslant y \leqslant n+1$. 当 m 和 n 遍取一切整数值时, 这个正方形的复本就构成整个平面的一个铺砖结

构 (tessellation, 或者说平面被铺上了砖, tiled 或 tesellated 两词均来自拉丁文的 tesslation 一词, 意为铺成一个镶嵌图的小石块), 而在每一个坐标为整数的点, 有 4 个正方形相会. 如果把这些小正方形黑白相间地图上颜色, 就会得到一个无限大的国际象棋棋盘.

要做一个环面, 就需要把某些不同的点等同起来. 我们说点 $(x\,,\,y)$ 和 $(x'\,,\,y')$ 相应于某个新图形上的同一点, 如果 $x-x'$, $y-y'$ 都是整数. 要想看一下这个新图形究竟是什么样, 就要注意, 平面上的每个点都相应于原来的正方形的一个内点或边界上的点. 此外, 如果 x 和 y 都不是整数, 则 $(x\,,\,y)$ 相应于正方形的恰好一个内点. 所以新图形看起来很像原来的正方形. 但是 $(1/4\,,\,0)$ 和 $(1/4\,,\,1)$ 这两个点又如何? 它们相应于新图形的同一点, 原来的正方形的上下对边的相应点也都相应于新图形的同一点. 所以, 在新图形中, 要把原来正方形的上下两边等同起来. 用类似的论证知道左右两对边也要等同起来. 因此当把各个点按上述规则等同以后, 就得到了环面.

如果这样作出了环面, 就可以这样来在环面上作图: 只要在原来的正方形上作图, [再把相应点等同起来就行了]; 正方形上的长度与环面上的长度相应, 而且准确地相等. 老式的滚筒印刷机就是这样工作的: 滚筒上涂了油墨的图形滚过纸张, 就印出了完全一样的图形. 这样, 就小图形而言, 环面上的几何学就是欧几里得几何学. 用数学语言就说, 环面上的几何学是由平面上的几何学诱导而来, 所以环面是**局部欧几里得**的. 当然, 整体而言二者很不相同, 例如在环面上, 可以作出不能收缩为一点的封闭曲线, 而在平面上就不会有这种事情.

还要注意, 我们引进了一个群来为我们完成了大部分工作. 在现在的情况, 这个群就是整数对 $(m\,,\,n)$ 所成的群, 而定义 $(m\,,\,n)+(m'\,,\,n')=(m+m'\,,\,n+n')$.

环面和球面只不过是无穷多种以下的曲面中的两个例子, 这些曲面是封闭的 (就是说, 没有边缘) 又是紧的 (就是说它们在任何意义下也不会走向无穷). 其他的例子则有: 两个孔的环面, 以及更一般的具有 n 个孔的环面 (即亏格为 $2, 3, 4, \cdots$ 的曲面). 要想类似地生成这些曲面, 就要用到**富克斯群**.

我们自然会期望, 利用多于 4 边的多边形就能得出其他曲面. 结果是, 如果利用 8 边形, 例如正 8 边形, 并把边 1 和 3 粘在一起, 2 和 4 粘在一起, 5 和 7 粘在一起, 6 和 8 粘在一起, 就会得到一个具有两个孔的环面. 我们怎样用群来做这件事, 就如刚才对于环面所做的那样? 为此我们需要有一种方法, 把许多 8 边形连到一起, 使得它们只在边上相接. 问题在于我们不能用 8 边形来作出平面的铺砖结构: 正 8 边形的顶角为 $135°$. 这个角太大了, 不可能把 8 个正 8 边形在一点粘到一起.

这里前进的道路是采用*双曲几何学*[I.3 §6.6] 来代替欧几里得几何学. 但是, 我们可以徒手来做这件事. 在复平面上取单位圆盘 $D=\{z:|z|=1\}$. 取所谓莫比乌斯 (August Ferdinand Möbius, 1790 –1868, 德国数学家) 变换的群, 而莫比乌斯变

换, 就是形如 $z \mapsto (az+b)/(cz+d)$ 的映射. 经过常规的计算就知道, 这些变化把圆周和直线映为圆周和直线 (这两种曲线要视为同一种, 所以圆周也可以被映为直线, 或者相反), 它们把角映为大小相等①[而且方向也相同的角. 还有一些变换是把角映为大小相等但符号相反的角, 好像平面上的反射那样]. 如果取把 D 映为自身的莫比乌斯变换, 就得到一个群, 记为 G. 事实上, 我们已经很接近于富克斯群了.

我们要找一个图形, 使它在这里起到正方形在欧几里得平面上所起的作用. [正如我们在上面把圆周和直线视为相同曲线一样, 现在视 D 的直径和垂直于 D 的边缘的圆弧为相同的曲线], 则 G 中的元素映垂直于 D 的边缘的圆弧 (包括直径) 为垂直于 D 的边缘的圆弧 (包括直径). 我们以后就以垂直于 D 的边缘的圆弧 (包括直径) 为直线, [其实是非欧几里得的直线], 并以 8 条这样的非欧几里得直线为边作出 (非欧几里得) 八边形. 这种八边形的作法有许多, 我们要选择最具对称性的一种, 使得以后事情更加容易. 即要画一个以 D 的中心为心的 "正八边形". 这里还有进一步选择的余地, [因为按照双曲几何学中多边形的角的亏值正比于其面积的著名定理], 八边形面积越大, 其顶角就越小, 我们要画的是顶角为 $\pi/4$ 的正八边形, 这样一来就可以让 8 个这样的正八边形汇聚在一个顶点处, 这就是我们需要的正八边形. 如果我们把不同的多边形在不同位置的相应的点等同起来, 所得的图形就是一个亏格为 2 的*黎曼曲面*[III.79].

富克斯群就是群 G(即变 D 为其自身的莫比乌斯变换所成的群) 的这样的元所成的子群. 这些元能把上面得到的正八边形 "整块地"(en bloc) 移动, 使得我们就能做出 D 的一个铺砖结构. 和在环面的情况一样, 现在也有了等价点 (即在不同 "砖块" 中占有相应位置上的点) 的概念, 当把等价的点等同起来以后, 就会得到最前面说的把多边形的不同的边粘连起来得到的图形. 这就是我们需要的图形.

所有这些都可以用双曲几何学的语言来描述. [我们得到的将是双曲几何学的**圆盘模型**], 它也可以用 D 上的一种*黎曼度量*[I.3 §6.10] 来定义, 这个度量就是

$$\mathrm{d}s = \frac{|\mathrm{d}z|}{\sqrt{1-|z|^2}}.$$

G 的元素将把图形在 D 中移来移去, 但保持双曲距离不变. 由此可知, 在新的曲面 (即把不同的对应点等同起来得到的图形) 上得到的几何学是局部双曲的几何学, 正如在环面上得到的几何学是局部欧几里得几何学一样.

因此, 如果从正 $4n$ $(n > 2)$ 边形开始, 并按上面的方法进行, 就会得到亏格为 n 的黎曼曲面. 但是数学家们能做的事情还更多. 如果回到平面, 但是不从正方形开始, 而从矩形开始, 或者更加一般地从平行四边形开始, 想要看出上面的做法可以继续实行下去, 这不算太难. 事实上, 如果从一个适当的角度来看平面, 而不是从

①原书说是符号相反的角犹如反射, 这句话错了, 莫比乌斯变换不是反射. —— 中译本注

平面的铅直上方来看这个平面, 则正方形也就会变成任意选择的平行四边形 (可能会放大或缩小一点). 如果用的是平行四边形, 仍然会得到一个环面, 不过与最早得到的环面不同, 其区别正如正方形和平行四边形的区别一样: 顶角的大小发生了变化. 下面是一个不算是完全平凡不足道的习题: 证明平行四边形的保持顶角大小不变的映射只能是相似变换 (就是在两个独立的方向上缩放的比例相同, 从而在一切方向上缩放比例相同的变换). 所以得出的环面在什么角度上有不同的意义, 就是说, 这样得出的环面与原来的环面有不同的**共形结构**.

在双曲圆盘上也会发生同样的事. 如果取一个 $4n$ 边多边形 (它的边是一段测地线), 而且其边长成对地相等, 并能找到一个群, 其元素能把这些多边形成块地移动, 使得适当的边准确地相配, 则又会得到一个黎曼曲面. 但是, 若这些多边形不是共形等价的, 则所得黎曼曲面也会有不同的共形结构. 甚至还可以向前再走一步, 允许某些顶点位于圆盘的边缘上, 这时, 多边形的相应的边的长度在双曲度量下将会是无穷大. 这样得到的图形是 “挖掉一点” 的黎曼曲面, 而数学家们又可以改变它的共形结构.

富克斯群的基本重要性来自**单值化定理**, 这个定理指出, 除了最简单的以外, 所有的黎曼曲面都是按照上述方式来自某个富克斯群. 这里面包括了所有亏格大于 1 的黎曼曲面和所有亏格为 1 但挖掉了一点的黎曼曲面, 并允许它们具有任意可能的共形结构.

富克斯群这个名词是*庞加莱*[VI.61] 在 1881 年给出的, 那时, 他正在研究超几何方程和相关的微分方程, 而这是受到了德国数学家富克斯 (Immanuel Lazarus Fuchs, 1833–1902) 的工作的启发. *克莱因*[VI.57] 提出了抗议, 认为以施瓦兹 (Karl Hermann Amandus Schwarz , 1843 –1921, 德国数学家) 命名更好, 庞加莱在读了施瓦兹相关的文章以后, 本来也准备同意这样做, 但是那时, 富克斯也已经赞成用这个名字. 但是克莱因的抗议有点过分 (在庞加莱看来如此), 于是庞加莱又把研究 3 维单位球体的共形映射所产生的一个类似的群公开称为克莱因群. 这些名字一直沿用至今. 但是克莱因群的研究要困难得多, 而克莱因和庞加莱对此都没有能做多少事情. 但是每一个黎曼曲面都来自球面或者欧几里得平面或者双曲平面, 这是他们二人都具有的猜测. 但是严格的证明, 直到 1907 年才由庞加莱和寇贝 (Paul Koebe, 1882–1945, 德国数学家) 独立地给出.

富克斯群的形式定义如下: 所有莫比乌斯变换所成的群的一个子群 H 称为不连续作用的, 如果对于圆盘 D 的每一个紧集合 K, $h(K)$ 和 K 都是互相分离的, 除了对于有限多个 $h \in H$ 例外. **富克斯群**就是所有的不连续作用于 D 的莫比乌斯变换所成的群.

III.29 函数空间

(Function Spaces)

陶哲轩 (Terence Tao)

1. 什么是函数空间?

当我们处理实数或复数时, 一个数 x 有一个自然的大小概念, 即它的模 $|x|$. 我们也可以利用这一个大小的概念来定义两个数 x 和 y 的距离 $|x-y|$, 由此可以说, 哪些成对的数是互相接近的, 哪些是远离的.

然而, 当处理具有较多自由度的对象时, 情况就变得比较复杂. 举例来说, 考虑决定一个 3 维矩形箱子的 "大小". 这里有好几个量可供选用: 长、宽、高、体积、表面积、直径 (最长的对角线长度)、扁平率等等. 不幸的是, 用这些量作出的大小比较并不是等价的. 例如, 箱子 A 可能比箱子 B 长一些, 而且体积也比较大, 但是箱子 B 可能宽一些, 而且表面积大一些. 由于这个原因, 人们放弃了箱子应该只用一个量来表示其大小的想法, 而接受了另一个思想: 有许多这样的大小概念, 它们都可能是有用的, 在有些应用里, 把大体积的箱子和小体积的箱子分开来; 在有些应用里, 可能想把扁平的箱子和圆一点的箱子分开来. 当然, 不同的大小概念有一些关系 (例如等周不等式[IV.26]). 它们在已知表面积时, 对体积的可能值给出了一个上界[①], 所以, 情况并不像初看起来那样漫无头绪.

现在回到具有固定的定义域和值域的函数 (最好心里记住一个定义在区间 $[-1, 1]$ 上而值在实直线 $\mathbf{R}$ 中的函数 $f:[-1,1]\to\mathbf{R}$, 这是一个好的例子). 这些对象有无穷多自由度, 所以毫不奇怪, 这里也有无穷多不同的 "大小" 概念, 而它们都对于 "一个已给的函数有多大" 这个问题 (或者对一个密切相关的问题: "两个函数 f 和 g 有多么接近?") 提供了不同的答案. 有时候, 一些函数在某种度量下有无穷的大小, 而在另一种度量下则只有有限大小 (类似地, 一对函数可能在某种度量下非常接近, 而在另一种度量下距离很远). 这里的情况又可能看起来很混乱, 但是它仅是反映了一个事实, 即函数可能有许多不同的特性 —— 有的高, 有的胖, 有的光滑, 有的震荡, 等等, 而按照不同的应用, 可能更着重于一种特性, 而不是另一种. 在分析里, 这些特性都体现在种种标准的**函数空间**及其相关的**范数**上, 而这些范数, 既可定量也可定性地描述这些函数.

形式地看, 一个函数空间常是一个赋范空间[III.62]X, 其元素是一些函数 (具有固定的定义域和值域). 在分析中考虑的标准的函数空间绝大多数 (但肯定不是全部) 不仅是赋范空间, 还是巴拿赫空间[III.62]. X 中的函数 f 的范数 $\|f\|_X$ 就是这

① 原书作上极限, 实际上等周不等式并未涉及极限问题, 所以改动了.—— 中译本注

个函数空间量度这个函数 f 有多大的方法. 通常 (但非一定如此) 范数是由简单的公式给出的, 而空间 X 就是由那些使得 $\|f\|_X$ 有意义并且为有限的函数构成的. 这样, 仅就函数 f 属于函数空间 X 这一事实, 就已经传递了关于这个函数的定量[①]的信息了. 例如, 它可能包含了 f 正规到**何种**程度[②], 它衰减**多么快**, 它以**什么常数**为界, 或者它的积分有**多大**, 等等.

2. 函数空间的例子

现在给出一些常用的函数空间的样本. 为简单起见, 仅限于考虑由 $[-1\,,\,1]$ 到 $\mathbf{R}$ 的函数的空间.

2.1 $C^0\,[-1\,,\,1]$

这个空间由所有由 $[-1\,,\,1]$ 到 $\mathbf{R}$ 的*连续函数*[I.3§5.5] 构成, 通常记作 $C[-1,1]$. 连续函数已经足够正规, 足以避免那些很粗糙的函数所产生的许多技术上微妙的地方. 紧[III.9] 区间 (如 $[-1\,,\,1]$) 上的连续函数是有界的, 所以可以加于这个空间的最自然的范数是**上确界范数**, 即 $|f|$ 的最大值, 记作 $\|f\|_\infty$(形式上说, 它的定义是 $\sup\{|f(x)|: x\in[-1\,,\,1]\}$), 但是对于连续函数, 说最大值或者说上确界, 是一致的.

上确界范数是与一致收敛性相联系的范数: 一个序列 $f_1\,,\,f_2\,,\cdots$ 一致收敛于 f, 当且仅当 $\|f_n-f\|$ 随 $n\to\infty$ 而趋于 0. 空间 $C^0\,[-1\,,\,1]$ 有一个有用的性质, 即其中的元素不但可以相加, 而且可以相乘, 这就使 $C^0\,[-1\,,\,1]$ 成为**巴拿赫代数**的最基本的例子.

2.2 $C^1\,[-1\,,\,1]$

这是一个对成员的资格限制比 $C^0\,[-1,\,1]$ 更严的空间: $C^1\,[-1\,,\,1]$ 中的函数 f 不仅是连续的, 而且它的导数在 $[-1\,,\,1]$ 上也是连续的. 上确界范数现在不是一个自然的范数, 因为一个连续可微函数序列可以在 $C^0\,[-1\,,\,1]$ 范数下收敛于一个不可微的函数. 现在应该定义 C^1**范数**$\|f\|_{C^1[-1\,,\,1]}$ 为 $\|f\|_\infty+\|f'\|_\infty$.

注意 C^1 范数现在不仅量度函数本身的大小, **还量度了**其导数的大小 (但是仅仅管住导数也不能令人满意, 因为那会给常值函数以零范数). 因此这是一个保证了比上确界范数更高的正规性的范数. 可以类似地定义二次连续可微的函数的空间 $C^2\,[-1\,,\,1]$ 等等, 一直到无穷可微函数的空间 $C^\infty\,[-1\,,\,1]$, [但是最后这个空间并不是赋范空间](这些空间还有"分数阶"的版本, 例如 $C^{0,\alpha}\,[-1\,,\,1]$, 即满足 α 阶赫尔德 (Otto Ludwig Hölder, 1859 –1937, 德国数学家) 条件的函数的空间. 本文不讨论这些变体).

---

① 原书作"定性"似与下文矛盾.—— 中译本注

② 一个函数的变动越光滑, 就认为它越正规.

2.3 勒贝格空间 $L^p[-1,1]$

上面给出的上确界范数 $\|f\|_\infty$ 对于所有的 $x\in[-1,1]$ 管住了 $|f(x)|$ 的大小. 然而, 这意味着如果有 x 的一个很小的集合, 使得 $|f(x)|$ 在其上很大, 则 $\|f\|_\infty$ 也会很大, 哪怕对于典型的 x, $|f(x)|$ 会小得很多. 有时, 取一个不那么受函数在小的集合上的值影响的范数会更加有利. 函数 f 的 L^p 范数是

$$\|f\|_p=\left(\int_{-1}^{1}|f(x)|^p\,\mathrm{d}x\right)^{1/p}.$$

当 $1\leqslant p<\infty$ 时, 它对于 [使得上面的积分有限的] 可测函数有意义. 这些函数构成 $L^p[-1,1]$ 空间. 可测函数 f 的范数 $\|f\|_\infty$ 是它的**本质上确界**, 这个概念粗略地说, 就是在函数的定义域中略去了一个测度为 0 的集合, 然后求此函数在此零测度集合的余集合上的上确界, 最后再求这些上确界的下确界. 那些使得 $\|f\|_\infty$ 保持有限的函数构成一个函数空间, 记作 $L^\infty[-1,1]$. [如果此函数是连续的, 则在定义域中略去一个 0 测度集合, 不会影响其上确界, 所以 $L^\infty[-1,1]$ 空间中的范数记号, 与 $C^0[-1,1]$ 空间中的 $\|f\|_\infty$ 是一致的. 在一般的文献中就不对记号作区别了]. 可以证明, 当 $p\to\infty$ 时, $\|f\|_\infty$ 是 $\|f\|_p$ 的极限. 可以说, $L^\infty[-1,1]$ 范数量度的是函数的 "高度", 而 L^p 范数量度的是函数的 "高度" 和 "宽度" 的综合.

这些范数中, 特别重要的是 L^2 范数, 因为 $L^2[-1,1]$ 是一个希尔伯特空间 [III.37]. 这个空间有特别丰富的对称性：存在非常丰富的种种**酉变换**, 即定义在 $L^2[-1,1]$ 上并且仍然映它到 $L^2[-1,1]$ 的使得 $\|Tf\|_2=\|f\|_2$ 的可逆线性变换 T.

2.4 索伯列夫空间 $W^{k,p}[-1,1]$

勒贝格范数在一定程度上控制了函数的高度和宽度, 但是对于函数的正规性未置一词; 一个 L 函数没有理由是可微的, 甚至没有理由是连续的. 为了把这些信息也放进来, 我们要转到**索伯列夫**(Sergei Lvovich Sobolev, 1908–1989, 前苏联数学家)**范数** $\|f\|_{W^{k,p}[-1,1]}$, 这里 $1\leqslant p\leqslant\infty$, $k\geqslant 0$. 其定义是

$$\|f\|_{W^{k,p}[-1,1]}=\sum_{j=0}^{k}\left\|\frac{\mathrm{d}^j f}{\mathrm{d}x^j}\right\|_p.$$

索伯列夫空间 $W^{k,p}[-1,1]$ 就是使得这种范数为有限的函数所成的空间. 这样, 一个函数在 $W^{k,p}[-1,1]$ 中当且仅当它和它的直到 k 阶的导数都在空间 $L^p[-1,1]$ 中. 这里有一点细微之处：我们并不要求 f 在通常意义下 k 次可微, 而是在较弱的分布[III.18] 的意义下 k 次可微. 例如, 函数 $f(x)=|x|$ 在零点并不可微, 但是它确有一个自然的弱导数：当 $x<0$ 时, $f'(x)=-1$, 当 $x>0$ 时, $f'(x)=1$. 这个函数属于 $L^\infty[-1,1]$(因为集合 $\{0\}$ 的测度为 0, 所以不必指定 $f'(0)$ 之值. 所以 f 属

于 $W^{1,\infty}[-1,1]$(这个空间就是**利普希茨连续函数**所成的空间). 我们需要考虑这些广义可微的函数, 因为否则空间 $W^{1,\infty}[-1,1]$ 将不是完备的.

在对偏微分方程和数学物理作分析研究时, 索伯列夫范数特别有用. 例如 $W^{1,2}[-1,1]$ 范数可以解释为与此函数相联系的 "能量"(的平方根).

3. 函数空间的性质

函数空间的构造在许多方面有助于研究函数. 例如, 如果在函数空间中有了一个好的基底, 使得此空间的每一个函数都可以写成这个基底的 (可能是无穷的) 线性组合, 而且对于这个线性组合如何收敛于原来的函数有一些定量的估计, 这就使我们能有效地用一些系数来表示这个函数, 而且可以用更光滑的函数来逼近它. 例如, 关于 $L^2[-1,1]$ 的一个基本的结果是, [从条目**傅里叶变换**[III.27] 里面讲到的**普兰舍利恒等式** 可以得出的]**普兰舍利定理**指出, 除了其他结果外, 还有: 存在复常数序列 $\{a_n\}_{n=-\infty}^{\infty}$ 使得当 $N\to\infty$ 时,

$$\left\|f-\sum_{n=-N}^{N}a_n\mathrm{e}^{\pi inx}\right\|\to 0\,.$$

这个结果表明, $L^2[-1,1]$ 中的任意函数都可以在 L^2 中用**三角多项式**, 即形如 $\sum_{n=-N}^{N}a_n\mathrm{e}^{\pi inx}$ 的表达式, 逼近到任意精确度. 这个复数序列中的 a_n 就是 f 的第 n 个**傅里叶系数** $\hat{f}(n)$, 它们可以用下面的公式来表示:

$$\hat{f}(n)=\frac{1}{2}\int_{-1}^{1}f(x)\,\mathrm{e}^{-\pi inx}\,\mathrm{d}x\,.$$

可以认为, 这个结果说的就是函数序列 $\mathrm{e}^{\pi inx}$, $n\in\mathbf{Z}$ 构成 $L^2[-1,1]$ 的很好的基底 (实际上, 它们构成规范正交基底, 即每个元素的范数均为 1, 而且任意两个不同元素的内积都是零).

关于函数空间的另一个很基本的事实是, 有些函数空间可以嵌入其他函数空间, 所以这个空间的所有函数自动地也属于另一个空间. 进而, 时常存在一个不等式, 用另一函数空间的范数来给出此函数空间范数的上界. 例如, 一个高正规性空间如 $C^1[-1,1]$ 的函数自动地属于一低正规性空间如 $C^0[-1,1]$, 而一个高可积性空间如 $L^\infty[-1,1]$ 中的函数自动地属于一个低可积性空间如 $L^1[-1,1]$(注意, 如果把区间 $[-1,1]$ 代以具有无穷测度的区间例如实数直线, 则这个命题不成立). 这些包含关系不能反转过来. 然而, 确实有所谓**索伯列夫嵌入定理**, 使我们能以正规性 "**交换**" 可积性. 这种结果告诉我们, 具有很多正规性但是可积性不足的空间, 可以嵌入到具有低正规性但是高可积性的空间里面. 下面这种估计

$$\|f\|_\infty\leqslant\|f\|_{W^{1,1}[-1,1]}$$

就是这种定理的一个样本. 它告诉我们, 如果 $|f(x)|$ 和 $|f'(x)|$ 的积分都有限, 则函数 f 必定是有界的 (这个结果比 $\|f\|_1$ 有限要强得多).

再一个非常有用的概念是对偶性[III.19] 的概念. 给定一个空间 X, 就可以定义其对偶空间 X^* 为 X 上的所有**连续线性泛函**的空间, 或者更精确地说, 就是所有的映射 $\omega: X \to \mathbf{R}$(或当函数空间中的函数取复值时为 $\omega: X \to C$) 之空间, 不过要求它们是线性的, 而且对于 X 的范数是连续的. 例如, 当 $1 < p < \infty$ 时, 可以证明实的 $L^p[-1, 1]$ 空间上的每一个线性泛函都可以用一个 $L^q[-1, 1]$ 的函数 g 写为

$$\omega(f) = \int_{-1}^{1} f(x)\, g(x)\, \mathrm{d}x,$$

这里的 q 由等式 $1/p + 1/q = 1$ 决定, 称为 p 的**共轭指数**.

要研究某函数空间的一个函数, 有时可以看对偶空间中的连续线性泛函如何作用于这些函数来进行. 类似于此, 要研究一个从一个函数空间 X 到另一个函数空间 Y 的连续线性算子 $T: X \to Y$, 有时也可以先考虑伴算子 $T^*: Y^* \to X^*$ 来进行, 这里 T^* 把 Y^* 之元 ω, 即 Y 上的连续线性泛函 $\omega: Y \to \mathbf{R}$ 映为 X^* 之元 $T^*\omega$, 其定义是: 对于 X 的任意元 x, 定义 $(T^*\omega)(x) = \omega(Tx)$.

关于函数空间, 我们还要提一个重要的事实, 某个函数空间 X 可以 "插入" 另外两个函数空间 X_0 和 X_1 中间. 例如空间 $L^p[-1, 1]$, $1 < p < \infty$ 以一种很自然的意义插入 $L^1[-1, 1]$ 和 $L^\infty[-1, 1]$ 中间. 插入的精确定义过于技术化, 所以本文不作解释, 但是关于它的所谓 "插值定理" 之所以很有用, 是因为有这样一个事实: "极端" 的空间 X_0 和 X_1 时常比 "夹在中间的" 空间更容易研究. 例如, 可以用它来给出**杨**(William Henry Young, 1863 – 1942, 英国数学家)**的不等式**以一个初等证明. 这个不等式就是说, 令 $1 \leqslant p, q, r \leqslant \infty$ 满足关系式 $1/p + 1/q = 1 + 1/r$, 而 f, g 分别属于 $L^p(\mathbf{R})$, $L^q(\mathbf{R})$, 令 $f * g$ 是 f 和 g 的卷积, 即有 $f * g(x) = \int_{\mathrm{R}} f(y)\, g(x-y)\, \mathrm{d}y$, 这时,

$$\left(\int_{-\infty}^{\infty} |f * g(x)|^r \,\mathrm{d}x\right)^{1/r} \leqslant \left(\int_{-\infty}^{\infty} |f(x)|^p \,\mathrm{d}x\right)^{1/p} \left(\int_{-\infty}^{\infty} |g(x)|^q \,\mathrm{d}x\right)^{1/q}.$$

插值定理在这里是很有用的, 因为在 $p = 1, q = 1$ 或 $r = \infty$ 这些极端的情况下, 这个不等式很容易证明. 如果不借助于插值定理, 这个证明就难多了.

III.30 伽 罗 瓦 群
(Galois Groups)

给定一个具有有理系数的多项式函数 f, 它的**分裂域**(splitting field) 就是包含所有有理数和 f 的所有的根的最小域[I.3 §2.2]. f 的伽罗瓦群则是分裂域的所有

自同构[I.3 §4.1] 的群. 每一个这种自同构都会把 f 的根加以排列, 所以伽罗瓦群可以看作所有这些根的置换群[III.68] 的子群. 伽罗瓦群的结构和性质与多项式的可解性密切相关. 特别是伽罗瓦群可以用来证明并非所有多项式都可以用根式来解出(就是用只包含通常的算术运算和开方的公式来表示解). 这个定理, 虽然看起来已经是一大奇观, 却并不是伽罗瓦群的仅有的应用, 它们在现代的代数数论中起了中心的作用.

关于更多的情况, 请参看五次方程的不可解性[V.21] 和代数数[IV.1§20].

III.31 Gamma 函数 (The Gamma Function)

Ben Green

若 n 是一个正整数, 则定义它的阶乘为乘积 $1\times2\times\cdots\times n$, 并记为 $n!$, 所以阶乘就是一直到 n 的正整数的乘积. 例如, 前 8 个阶乘就是 1, 2, 6, 24, 120, 720, 5040, 以及 40 320 (用惊叹号表示阶乘, 始自 Christian Kramp, 至今已有 200 多年了, 当时是为了印刷者的方便, 也许是因为要传递一种对于 $n!$ 增长之快的惊异之情. 在有些 20 世纪的文献中, 仍然在使用一种过时的记号 $\underline{n|}$). 从定义来看, 似乎对于不是正整数的数, 定义阶乘是不可能的, 然而, 结果是这样做不仅可能而且极为有用.

Gamma 函数记作 $\Gamma(x)$, 当 x 为正整数时, 就是阶乘函数, 但是对于任意的实数甚至是复数 x 都是有意义的. 事实上, 当 $n=2$, 3 , $\cdots$ 时, 定义 $\Gamma(n)=(n-1)!$ 是很自然的. 让我们一开始先把 Gamma 函数写成

$$\Gamma(s)=\int_0^\infty x^{s-1}\mathrm{e}^{-x}\mathrm{d}x\,, \tag{1}$$

而暂时不管积分是否收敛. 分部积分后, 就有

$$\Gamma(s)=\left[-x^{s-1}\mathrm{e}^{-x}\right]_0^\infty+\int_0^\infty(s-1)\,x^{s-2}\mathrm{e}^{-x}\mathrm{d}x\,. \tag{2}$$

当 $x\to\infty$ 时, $x^{s-1}\mathrm{e}^{-x}$ 趋于零, 而若 s 例如是一个比 1 大的实数时, 当 $x=0$ 时, 也有 $x^{s-1}=0$. 所以对于这种 s, 上式右方第一项为 0, 而第二项正是 $\Gamma(s-1)$, 所以证明了 $\Gamma(s)=(s-1)\Gamma(s-1)$. 如果想把 $\Gamma(s)$ 看成与阶乘 $(s-1)!$ 类似的东西, 这正是我们需要的公式.

不难证明, 如果 s 是一个实部 $\mathrm{Re}(s)$ 为正的复数时, 这个积分确实是收敛的. 此外, 它在这个区域中定义一个全纯函数[I.3 §5.6]. 当 s 的实部为负时, (1) 中的积分根本不收敛, 所以不能用它来定义 Gamma 函数. 但是可以用 $\Gamma(s)=(s-1)\Gamma(s-1)$ 来拓展 Gamma 函数的定义区域. 例如, 如果 $-1<\mathrm{Re}(s)\leqslant0$, 我

们知道以积分 (1) 作为定义是不能直接应用的, 但是若在 (1) 中把 s 换成 $s+1$, 则可以使用积分 (1) 作为定义, 因为现在 $\mathrm{Re}\,(s+1)>0$. 我们知道 $\Gamma(s+1)=s\Gamma(s)$, 所以, 如果现在定义 $\Gamma(s)$ 为 $\Gamma(s+1)/s$, 则 $\Gamma(s)$ 也有定义. 一旦我们做完了这一点, 则可以仿此进一步考虑 s 之值适合 $-2<\mathrm{Re}\,(s)\leqslant-1$ 的情况, 以下类推.

但是读者可能会对例如 $s=0$ 的 $\Gamma(0)$ 的情况持反对意见, 因为这里用零作了分母. 然而, 现在这是完全许可的, 因为我们要求于 $\Gamma(s)$ 的, 只是它是一个亚纯函数[V.31], 而亚纯函数是允许取 ∞ 为"值"的. 事实上, 不难看到, 我们所定义的 Gamma 函数在 $0,-1,-2,\cdots$ 处有单极点.

事实上有许多函数具有与 Γ 同样有用的性质 (例如, 因为对任意的 s, $\cos(2\pi s)=\cos(2\pi(s+1))$, 而且对任意整数 n, 都有 $\cos(2\pi n)=1$, 所以函数 $F(s)=\Gamma(s)\cdot\cos(2\pi s)$ 也具有 $F(s)=(s-1)F(s-1)$ 以及 $F(n)=(n-1)!$). 然而, 由于种种理由, 我们所定义的 Γ 函数是阶乘函数的最自然的亚纯函数推广. 这样说, 最有说服力的理由是它在自然的背景下出现得最频繁, 而且在一定意义下, 它是阶乘函数到所有正实数的最光滑的插值. 事实上, 如果 $f:(0,\infty)\to(0,\infty)$ 适合以下关系式: $f(x+1)=xf(x)$, $f(1)=1$, 而且 $\log x$ 是凸函数, 则 $f=\Gamma$.

有许多涉及 Γ 函数的有趣的性质, 例如 $\Gamma(s)\Gamma(1-s)=\pi/\sin(\pi s)$. 还有著名的结果 $\Gamma\left(\frac{1}{2}\right)=\sqrt{\pi}$, 它在本质上等价于下面这个事实: "正态分布曲线" $h(x)=(1/\sqrt{2\pi})\,\mathrm{e}^{-x^2/2}$ 下面的面积等于 1(只要在 (1) 式中作变换 $x=u^2/2$, 就可以看到这一点). 关于 Γ 还有一个重要的结果, 即魏尔斯特拉斯的无穷乘积公式, 即对复平面上所有的 z, 有

$$\frac{1}{\Gamma(z)}=z\mathrm{e}^{\lambda z}\prod_{n=1}^{\infty}\left(1+\frac{z}{n}\right)\mathrm{e}^{-z/n},$$

其中 γ 是欧拉常数,

$$\gamma=\lim_{n\to\infty}\left(1+\frac{1}{2}+\cdots+\frac{1}{n}-\log n\right).$$

这个公式使我们清楚地看到, Γ 不会等于 0, 而且在 0 和负整数处有单极点.

为什么 Gamma 函数这么重要? 一个足够简单的理由是它时常出现在许多数学分支里面. 但是, 我们还可以问, 为什么它时常出现在许多数学分支里? 理由之一是用 (1) 式所定义的 Γ 是自然的无可争辩的函数 $f(x)=\mathrm{e}^{-x}$ 的梅林变换, 梅林变换是一种类型的傅里叶变换[III.27], 但是它是关于定义在群 $(\mathbf{R}^+,\times)$ 上的函数的"傅里叶变换", 而不是关于定义在群 $(\mathbf{R},+)$ 上的函数的傅里叶变换 (那个群才是绝大多数函数的栖息地). 因为这个原因, 时常在数论 (特别是解析数论[IV.2]) 里面见到 Γ, 在那里, 用连乘积来定义的函数时常是通过求傅里叶变换来研究的.

Γ 在数论中有一次露面是在黎曼 ς 函数[III.80] 或 [IV.2§3] 中, 即

$$\Xi(s)=\Gamma(s/2)\,\pi^{-s/2}\varsigma(s)\ , \tag{3}$$

它适合关系式 $\Xi(s)=\Xi(1-s)$, 而 ς 函数有一个著名的无穷乘积表达式

$$\varsigma(s)=\prod_p\left(1-p^{-s}\right)^{-1},$$

这里的 p 是一切素数, 而这个式子对整个半平面 $\Re(s)>1$ 有效. (3) 中的因子 $\Gamma(s/2)\,\pi^{-s/2}$ 可以认为是来自 "无穷远处的素数"(这个名词可以严格地定义).

斯特林(James Stirling, 1692–1770, 英国数学家)**公式**是在处理 Γ 函数时常用的一个公式, 它提供了用较简单的函数去逼近 Γ 函数的一个相当精确的近似式. $n!$ 的一个粗糙的 (但是时常很有用的) 近似式是 $(n/\mathrm{e})^n$, 它告诉我们 $\log(n!)$ 大体上就是 $n(\log n-1)$. 斯特林公式就是这个粗糙估计的很大的改进. 令 $\delta>0$, z 则是一个复数, 其模至少是 1, 而幅角则在 $-\pi+\delta$ 和 $\pi-\delta$ 之间 (第二个条件使得 z 离开了负实轴, 而 Γ 函数的极点则全在负实轴上). 斯特林公式指出,

$$\log\Gamma(z)=\left(z-\frac{1}{2}\right)\log z-z+\frac{1}{2}\log 2\pi+E,$$

这里的误差 E 最多是 $C(\delta)/z$, 而 $C(\delta)$ 则是一个依赖于 δ 的正实数 (若取 δ 较小, 就必须取 $C(\delta)$) 更大. 利用此式就可以断定, 若令 z 在复平面的铅直带形中趋向无穷: $\mathrm{Im}z\to\infty$, 则 Γ 一定指数衰减. 事实上, 若 $\alpha<\sigma<\beta$, 则对所有的 $|t|>1$,

$$|\Gamma(\sigma+\mathrm{i}t)|\leqslant C(\alpha\ ,\ \beta)\,|t|^{\beta-1}\,\mathrm{e}^{-\pi|t|/2}$$

对 σ 一致地成立.

III.32 生成函数
(Generating Functions)

假设已经定义了一个组合结构, 而且想知道对每一个非负整数 n, 这个结构里面有多少大小为 n 的样本. 如果这个数目是 a_n, 则打算分析的就是序列 a_0 , a_1 , a_2 , a_3 , $\cdots$. 如果它的结构相当复杂, 这就可能是一个相当困难的问题. 但是有时如果考虑另外一个对象, 问题会容易一些, 这个对象就是序列的**生成函数**, 其中包含了和原序列同样的信息.

为了定义这个函数, 只需把这个序列看成是某一个幂级数的系数序列. 就是说, 一个序列的生成函数是由以下公式给出的:

$$f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + \cdots.$$

生成函数之所以有用, 是因为有时可以得到它的简洁的表达式, 只需分析这个表达式, 而不必参照个别的数 a_n. 例如有一个重要的生成函数是 $f(x) = (1-\sqrt{1-4x})/2x$. 这时, 就可以从生成函数的性质导出序列 a_0, a_1, a_2, $\cdots$ 的性质, 而不必反过来做.

关于生成函数, 可见列举组合学与代数组合学[IV.18] 与变换[III.91].

III.33 亏 格
(Genus)

亏格是曲面的一个拓扑不变量, 就是一个与曲面相关而且当曲面连续变形是不变的量. 粗略地说, 它相应于曲面上的洞的个数, 所以球面的亏格为 0, 环面的亏格为 1, 最简单的 "麻花" 就是一个吹胀了的 8 字形① 的亏格为 2, 等等. 若把一个可定向的曲面加以三角剖分, 并且记其顶点、棱与面的数目为 V, E 和 F, 则定义其欧拉示性数为 $V-E+F$, 并且记作 χ, 若记亏格为 g, 可以证明 $\chi = 2-2g$. [I.4 §2.2] 中有比较详细的讨论.

庞加莱[VI.61] 有一个著名的结果指出, 对每一个非负整数 g 都恰好有一个可定向的曲面以 g 为亏格 (进一步, 对于不可定向的曲面也可以定义亏格, 而且有类似的结果). 关于这个定理的详细说明可见微分拓扑[IV.7 §2.3].

可以把一个可定向曲面从而可以把一个亏格和一条光滑代数曲线联系起来. 一条椭圆曲线[III.21] 可以定义为一条亏格为 1 的光滑曲线. 详细的讨论可见条目代数几何[IV.4 §10].

III.34 图
(Graphs)

图是最简单的数学结构之一, 它由若干个 (通常为有限多个)**顶点**和某些顶点的对子组成, 这些顶点对就说是 "相连接的". 顶点通常用平面上的点来表示, 再用

① 原文是 pretzel, 这是一种油炸的小食品, 国内的读者未必见过, 说是麻花, 其实也不太像, 总之是组在一起的面条油炸而成. 说是 8 字形就准确了, 关键在于只有两个洞. —— 中译本注

线段把相连接的顶点对连接起来, 这些线段就叫做**边**(至于线段怎样画, 看起来是什么样, 都不重要, 重要的只是两个顶点是否相连接的).

例如, 一个国家的铁路网可以用一个图来表示: 用顶点来表示车站, 如果两个顶点是一条铁路紧接着的车站, 就说这两个顶点是连接的. 因特网是另一个例子, 顶点就是全世界的计算机, 如果两个计算机有直接的连接, 就说它们是相连接的.

图论中的许多问题取下面的形式: 图的结构的某些性质能推出哪些其他性质. 例如, 想要找出一个具有 n 个顶点但不包含三角形的图(三角形就是所有顶点都互相连接的顶点集合), 这样一个图有多少条边? 很明显, $\frac{1}{4}n^2$ 条边是可能的. 至少当 n 为偶数时如此, 这是因为这时可以把顶点分成各含相同数目顶点的两类. 把一类的每一个顶点都与另一类的每一个顶点连接起来, [但同类顶点则不要连接], 就成功了. 但是是否可能有更多的边呢?

下面是关于图的另一个典型问题的例子. 令 k 为一正整数, 是否一定存在一个正整数 n, 使得具有 n 个顶点的图中一定包含有 k 个顶点, 而它们的任意两个都是互相连接的, 或者包含 k 个顶点, 而其中任意两个都不连接?

关于这些问题 (第一个是 "极值图论" 的创始问题, 而第二个是 "拉姆齐理论" 的创始问题), 以及关于图的一般的研究, 可参看**极值与概率组合学**[IV.19].

III.35 哈密顿函数 (Hamiltonians)

陶哲轩 (Terence Tao)

初看起来, 现代物理学的许多理论和方程表现出令人眼花缭乱的多样性, 例如, 把经典力学与量子力学比较, 把非相对论物理与相对论物理比较, 或者把粒子物理和统计力学比较, 就可以看到这一点. 然而, 有许多强大的起统一作用的主题把它们联系起来, 其中之一就是在所有这些理论中, 物理系统随时间的演化 (以及这些系统的定常状态) 在很大程度上是受到一个单个的对象的控制, 即这个系统的**哈密顿函数**. 这个函数时常可以解释为这个系统的总能量. 大略地说, 每一个物理现象 (电磁现象、原子键、势阱中的粒子等等) 都对应于一个哈密顿函数 H, 而每一种类型的力学 (经典、量子、统计力学) 都相应于用这个哈密顿函数来描述一个物理系统的不同方法. 例如, 在经典物理中, 哈密顿函数确实是这个系统的位置 q 和动量 p 的函数: $(q, p) \mapsto H(q, p)$, 而 H 按照所谓哈密顿方程

$$\frac{\mathrm{d}q}{\mathrm{d}t} = \frac{\partial H}{\partial p}, \qquad \frac{\mathrm{d}p}{\mathrm{d}t} = -\frac{\partial H}{\partial q}$$

演化. 在 (非相对论的) 量子力学中, 哈密顿 "函数" 实际上是一个线性算子[III.50](位置算子 q 和动量算子 p 的一个形式组合), 而系统的波函数 ψ 则满足薛定谔方程[III.83]:

$$i\hbar\frac{\mathrm{d}}{\mathrm{d}t}\psi = H\psi.$$

在统计物理中, 哈密顿函数 H 则是系统的**微观态**(microstate) 的函数, 而系统在给定的温度 T 下处于这个微观态的概率则是 $\mathrm{e}^{-H/kT}$, 诸如此类, 等等.

数学的许多领域都与自己的物理对应物密切地缠在一起, 所以, 毫不奇怪, 哈密顿函数的概念也出现在纯粹数学里面. 例如, 受到经典物理的启发, 哈密顿函数 (及其下述的推广, 如**矩映射**(moment map)) 在动力系统、微分方程、李群理论、辛几何里面都起重要作用. 受到量子力学的启发, 哈密顿函数 (及其下述的推广, 如**可观测量**、**拟微分算子**) 在算子代数、谱论、表示理论、微分方程和微局部分析中同样也很突出.

因为哈密顿函数在那么多物理和数学领域里都出现, 它在建立表面上似乎无关的领域间的桥梁中就很有用, 例如, 建立经典力学与量子力学、辛力学和算子代数的联系. 一个给定的哈密顿函数的性质时常会揭示出与此哈密顿函数相关的物理或数学对象的众多性质. 例如, 哈密顿函数的对称性时常会诱导出用此哈密顿函数表示的对象的对称性. 虽然不能说一个数学或物理对象的所有有趣的性质都可以直接从它们的哈密顿函数读出, 但是在理解这些对象的性质和动态时哈密顿函数仍然起着基本的作用.

请参看顶点算子代数[IV.17 §2.1]、镜面对称[IV.16 §2.1.3, 2.2.1], 以及辛流形[III.88 §2.1].

III.36 热 方 程
(The Heat Equation)

Igor Rodnianski

热方程首先是由傅里叶[VI.25] 作为热在固体中传导的数学描述提出来的. 后来在数学的许多角落里都感到了它的影响. 它为下面这些相距甚远的现象提供了解释, 这里有冰的融化 (**施特藩问题**)、不可压缩粘性流理论 (纳维–斯托克斯方程[III.23])、几何流 (例如曲线的缩短、调和映射热流问题)、布朗运动[IV.24]、液体在多孔介质中的渗透 (**施特藩问题**) 指标定理 (如 **Gauss-Bonnet-Chern 公式**)、股票期权的定价 (Black-Scholes公式[VII.9 §2]、3 维流形的拓扑学 (庞加莱猜想[V.25]). 但是热方程的光明未来在它诞生的时候就已经被预见到了, 另一件随它而来的 "小事情" 是傅里叶分析[III.27] 的创立.

热的传导的研究是基于简单的连续性的考虑. 在一个小体积 ΔV 和一个小时段 Δt 内, 热量的变化是

$$CD\frac{\partial u}{\partial t}\Delta V\Delta t\,,$$

其中 C 是传热物质的热容量, D 是其密度, 而这个量又可以由计算通过 ΔV[的边缘 $\partial\Delta V$] 流入或流出 ΔV 的热量来得出, 因此它的近似值是

$$K\Delta t\int_{\partial\Delta V}\frac{\partial u}{\partial n}\mathrm{d}S\,,$$

[这里的 $\mathrm{d}S$ 是 $\partial\Delta V$ 的面积单元], K 是导热系数, n 则是 $\partial\Delta V$ 的内法线方向的单位向量.

现在假设所有的物理常数都等于 1. [令上面的两个积分相等, 再对第二个积分应用高斯定理], 然后用 $\Delta t\Delta V$ 遍除这两个积分, 并令 Δt 和 ΔV 都趋近 0, 就会得到控制一个 3 维物体 Ω 中热量 (以温度来表示)u 的演化的经典的热方程

$$\frac{\partial}{\partial t}u(t\,,\,x)-\Delta u(t\,,\,x)=0, \tag{1}$$

这里 $u(t\,,\,x)$ 是 Ω 中的点 $x=(x\,,\,y\,,\,z)$ 处在时刻 t 的温度, 而

$$\Delta=\frac{\partial^2}{\partial x^2}+\frac{\partial^2}{\partial y^2}+\frac{\partial^2}{\partial z^2}$$

是 3 维的拉普拉斯算子, 这个方程表示 Δu 就是

$$\frac{1}{\Delta V}\int_{\partial\Delta V}\frac{\partial u}{\partial n}\mathrm{d}S$$

当 ΔV 趋于 0 时的极限. 为了决定 $u(t\,,\,x)$, 对于方程 (1) 还要补充温度的**初始分布**[即 $t=0$ 时的温度]$u_0(x)=u(0\,,\,x)$, 以及在物体与外界的交界处 [即 Ω 的边缘]$\partial\Omega$ 上的**边界条件**. 例如, 若物体是单位立方体 C, 而在其表面上保持温度为 0, 这时就要考虑热方程的狄利克莱问题, 而傅里叶指出 $u(t\,,\,x)$ 可以用分离变量法解出, 即先把 $u_0(x)$ 展开为傅里叶级数

$$u_0(x\,,\,y\,,\,z)=\sum_{k,m,l=0}^{\infty}C_{kml}\sin(\pi kx)\sin(\pi my)\sin(\pi lz)\,,$$

而由此即可得出解为

$$u(t\,,\,x\,,\,y\,,\,z)=\sum_{k,m,l=0}^{\infty}\mathrm{e}^{-\pi^2\left(k^2+m^2+l^2\right)t}\sin(\pi kx)\sin(\pi my)\sin(\pi lz)\,.$$

这个简单的例子就已经说明了热方程的基本性质，它的解有收敛到定常状态的倾向. 在现在的情况，反映了一个物理上很直观的事实，即温度趋向于均匀的分布 $u^*(x) = C_{000}$.

绝缘物体中的热传导相应于选用**冯 · 诺依曼边界条件**，即要令温度的法向（即 Ω 的边缘 $\partial\Omega$ 的法线方向）导数为 0，它的解也可以用类似方法得出.

傅里叶分析与热方程有密切关系的原因是：三角函数是拉普拉斯算子的本征函数[I.3 §4.3]. 如果把拉普拉斯算子换成更一般的线性自伴算子[III.50 §3.2]，而且它具有正的哈密顿函数[III.35]([不过，在那里说过的，在这个情况下，哈密顿“函数”其实是一个算子，所以下面我们说哈密顿算子. 在傅里叶变换[III.27] 的一个脚注里说过，从这个角度来看，拉普拉斯算子应该取为 $-\Delta$ 才相应于哈密顿算子])H，就会得到许多更一般的热方程，它们具有离散的本征值 λ_n 的集合和相应的本征函数 ψ_n. 这样，热流的方程是 $\dfrac{\partial}{\partial t}u + Hu = 0$. 现在解就由公式 $u(t) = u(t, x, y, z) = \mathrm{e}^{-tH}u_0$ 给出，e^{-tH} 是由 H 生成的**热流半群**. 解也可以写成更加显式的式子

$$u(t, x) = \sum_{n=0}^{\infty} \mathrm{e}^{-\lambda_n t} C_n \psi_n(x),$$

这里的系数 C_n 是 u_0 相对于 H 的傅里叶系数，就是说，它们来源于把 u_0 展开为 $\sum\limits_{n=0}^{\infty} C_n\psi_n$(这种展开式的存在可由自伴算子的谱定理[III.50§3.4] 得出. 用类似的论证知道，热流也可以由具有连续谱的自伴算子生成). 特别是，$u(t, x)$ 当 $t \to \infty$ 时的渐近性态完全由 H 的谱来决定.

这些表达式虽然是显式的，却对热方程的性态没有给出很好的定量描述. 想要得到这样的描述，就得放弃显示地构造解这个思想，而转来寻找可以用于一般类型的解的原理和方法，这些原理和方法还得要充分有力而灵活多变，这样才能对于分析更复杂的热方程有用.

这种类型的方法第一个就是**能量恒等式**. 要想导出能量恒等式，先用某个量去乘热方程，这个量依赖于已给的解，然后再作分部积分. 这种类型的恒等式中，最重要的有二，其一是绝缘物体的**总热量守恒**：

$$\frac{\mathrm{d}}{\mathrm{d}t}\int_\Omega u(t, x)\,\mathrm{d}x = 0 ;$$

其二则是能量恒等式：

$$\int_\Omega u^2(t, x)\mathrm{d}x + 2\int_0^t \int_\Omega |\nabla u(s, x)|\mathrm{d}x\mathrm{d}s = \int_\Omega u^2(0, x)\mathrm{d}x .$$

第二个恒等式包含了热方程的一个基本的光滑化性质，因为 3 个积分都是非负的，而第一和第三个积分又都是有限的，所以 u 的梯度的平均平方平均值也是有限的，

哪怕梯度的初始的平均平方为无限时也如此, 而且, 当 t 趋向无穷大时, 这个平均平方值 [即第二个积分的内层积分] 甚至趋于 0. 事实上, 在离开 $\partial\Omega$ 处, 就会发生任意程度的光滑化, 不仅是对于时间的平均地光滑化, 而且是对于每一个时刻 $t>0$ 都发生光滑化.

热方程的第二个基本的原理是整体极值原理

$$\max_{x\in\Omega,0\leqslant t\leqslant T} u(t,x)\leqslant \max\left(u(0,x),\max_{x\in\partial\Omega,0\leqslant t\leqslant T} u(t,x)\right),$$

它所讲的其实是一个我们熟知的事实: 一个物体最热的点, 或者是发生在边缘上, 或者是发生在初始时刻.

最后, $\mathbf{R}^n$ 上的热方程的扩散性质包含在其非负解 u 的**哈纳克**(Carl Gustav Axel Harnack, 1851–1888, 德国数学家)**不等式**中. 这个不等式指出, 当 $t_2>t_1$ 时,

$$\frac{u(t_2,x_2)}{u(t_1,x_1)}\geqslant\left(\frac{t_1}{t_2}\right)^{n/2}\mathrm{e}^{-|x_2-x_1|^2/4|t_2-t_1|}$$

这个不等式告诉我们, 如果 x_1 处时刻 t_1 的温度取某个值, 则在以后, 即在 t_2 时, 不论哪一点 x_2 的温度都小不到哪里去.

这种形式的哈纳克不等式里出现了热方程的研究中的一个非常重要的对象: **热核**

$$p(t,x,y)=\frac{1}{(4\pi t)^{n/2}}\mathrm{e}^{-|x-y|^2/4t}.$$

它的众多应用之一是告诉我们如何用初始温度 $u_0(x)$ 来表示出热方程在全空间 $\mathbf{R}^n$ 的解, 这就是以下的公式

$$u(t,x)=\int_{\mathbf{R}^n}p(t,x,y)u_0(y)\,\mathrm{d}y.$$

它也告诉我们, 在时间 t 以后, 初始的扰动会分布到一个以初始扰动点为中心、半径为 $\sqrt{t}$ 的球体内. 这种空间尺度与时间尺度的关系是作为热方程的特征的抛物尺度化.

爱因斯坦曾指出, 热方程与布朗运动的扩散过程有密切的关系. 事实上, 布朗运动在数学上是用一个随机过程 B_t 来描述的, 其转移概率密度就是热核 $p(t,x,y)$. 对于从 x 开始的 n 维布朗运动 B_t^x, 用期望值来表示的函数

$$u(t,x)=E\left[u_0\left(\sqrt{2}B_t^x\right)\right]$$

就是热方程的以 $u_0(x)$ 为初始值的解. 这个式子正是热方程和概率理论的联系的起点, 而这个联系对于双方都大有好处. 在这种关系中, 最为有用的结果之一就是

Feymann-Kac 公式

$$u(t, x)=E\left[\exp\left(-\int_0^t V\left(\sqrt{2}B_s^x\right)\mathrm{d}s\right)u_0\left(\sqrt{2}B_t^x\right)\right],$$

它把布朗运动与具有初值 $u_0(x)$ 的 [推广了的] 热方程

$$\frac{\partial}{\partial t}u(t, x)-\Delta u(t, x)+V(x)u(t, x)=0$$

的解联系起来了.

上面所说的关于热方程的三个基本的原理引人注目地灵活多变, 就是说, 它们或者它们的较弱的形式, 甚至对于经典的方程的非常一般的变体都适用. 例如, 它们可以用于热方程

$$\frac{\partial}{\partial t}u-\sum_{i,j=1}^n\frac{\partial}{\partial x_i}\left(a_{ij}(x)\frac{\partial}{\partial x_j}u\right)=0$$

的解的连续性问题, 而这里对于系数 a_{ij} 只假设为有界, 并且满足椭圆性条件 $\lambda|\xi|^2\leqslant\sum_{i,j=1}^n a_{ij}\xi^i\xi^j\leqslant\Lambda|\xi|^2$, $0<\lambda$, Λ, 甚至可以考虑 "非散度形式" 的方程:

$$\frac{\partial}{\partial t}u-\sum_{i,j=1}^n a_{ij}(x)\frac{\partial}{\partial x_i}\frac{\partial}{\partial x_j}u=0.$$

这时, 热方程和随机扩散过程的联系变得特别有帮助. 这个分析在*变分法*[III.94] 和完全非线性问题中有特别美妙的应用.

对于*黎曼流形*[I.3 §6.10] 上的热方程, 这些原理也成立. 在黎曼流形 M 上, 拉普拉斯算子的适当的类似物是**拉普拉斯–贝尔特拉米**(Eugenio Beltrami, 1835–1900, 意大利数学家)**算子**Δ_M, 而 M 上的热方程则是

$$\frac{\partial}{\partial t}u-\Delta_M u=0.$$

如果 M 上的度量是 G, 则在局部坐标下

$$\Delta_M=\frac{1}{\sqrt{\det G(x)}}\sum_{i,j=1}^n\frac{\partial}{\partial x_i}\left(g^{ij}(x)\frac{\partial}{\partial x_j}\right).$$

这时, 对于具有下有界的*里奇曲率*[III.78] 的流形, 哈纳克不等式仍然成立. 人们对于流形上的热方程有兴趣, 部分地是由于希望了解非线性几何流及其长时间性态所引发的. 最早的几何流之一是**调和映射流**

$$\frac{\partial}{\partial t}\Phi-\Delta_M^N\Phi=0,$$

它描述两个紧黎曼流形 M 和 N 之间的映射 $\Phi(t,\cdot)$ 的变形. 算子 Δ_M^N 是一个非线性拉普拉斯算子, 是由将 Δ_M 投影到 N 的切空间作出来的. 它是相应于能量

$$E[U]=\frac{1}{2}\int_M |\mathrm{d}U|_N^2$$

的**梯度流**, 它量度了 M 和 N 之间的映射 U 的拉伸. 在 N 的**截曲率**(sectional curvature) 为非正的假设下, 可以证明调和映射热流是正规的, 而且当 $t\to\infty$ 时, 收敛于 M 和 N 之间的调和映射, 这个映射是能量泛函 $E[U]$ 的临界点. 这样, 热流被用来证明调和映射的存在, 以及构造一个已给的映射 $\Phi(0,\cdot)$ 的连续变形, 使之趋向于一个调和映射 $\Phi(\infty,\cdot)$. 对于目标流形 N 的曲率的假设是用于调和映射热流的关键性的**单调性性质**, 这个性质正是由于使用了能量估计而大白于天下.

这一类变形原理的一个更令人叹为观止的应用是用于*里奇流*[III.78]:

$$\frac{\partial}{\partial t}G_{ij}=-2\mathrm{Ric}_{ij}(G),$$

这是一个已给的流形 M 上的一族度量 $G_{ij}(t)$ 的拟线性热方程. 这时, 流不一定是正规的, 然而可以用 "割补术"(surgery) 把它扩充为一个流, 而对割补的结构和这个流的长时间动态都可以进行精确的分析. 特别是这个分析证明了任意的 3 维单连通流形都微分同胚与 3 维球面, 这就给出了庞加莱猜想的证明.

热方程的长时间性态对于反应扩散系统的分析也很重要, 这样又与生物现象有了联系. 这一点早在*图灵*(A.M. Turing)[VI.94] 的工作里就已经提到, [在图灵去世前几年], 他就试图了解**形态的发生**(morphogenesis)(例如, 怎样从近乎均匀的初始形态产生出如像动物皮毛的斑纹那种不均匀的**模式**(pattern)), 他试图用反应扩散方程组

$$\frac{\partial}{\partial t}u=\mu\Delta u+f(u,v),\quad \frac{\partial}{\partial t}v=\nu\sum v+g(u,v)$$

的指数不稳定性来解释这些现象.

这些例子都强调了热方程的长时间性态, 特别是它的解趋向收敛于平衡态或者产生出指数不稳定性. 然而事实证明, 流形 M 上的热方程的短期性态对于研究这个流形的几何和拓扑极为重要. 这里有两方面的联系, 首先, 人们希望建立 Δ_M 的谱与 M 的几何的联系; 其次, 可以用对于短期性态的分析来证明**指标定理**. 第一个方面, 在平面区域的背景下, 包含在卡茨的著名问题 **"您能够听出鼓的形状吗?"**[①] 对于一个流形, 这个问题首先从*外尔*[VI.80]**公式**

$$\sum_{i=0}^{\infty}\mathrm{e}^{-t\lambda_i}=\frac{1}{(4\pi t)^{n/2}}(\mathrm{Vol}(M)+O(t))$$

① 这个问题首先发表在一篇著名的论文中: Kac M. Can one hear the shape of a drum. *Amer. Math. Monthly*, 1966, 73(4), part II: 1-23.—— 中译本注

开始, 并考虑 $t \to 0$ 的情况. 式左是 Δ_M 的热核的迹, 即

$$\sum_{i=0}^{\infty} \mathrm{e}^{-t\lambda_i} = \operatorname{tr} \mathrm{e}^{-t\Delta_M} = \int_M p(t, x, x)\,\mathrm{d}x,$$

而 $p(t, x, y)$ 是这样的函数, 使得热方程 $\frac{\partial}{\partial t}u - \Delta_M u = 0$ 以及初始条件 $u(0, x) = u_0(x)$ 的解可以表示为

$$u(t, x) = \int_M p(t, x, y)\, u_0(y)\,\mathrm{d}y.$$

外尔恒等式的右方则反映了热核的短期性态.

指标定理的热流证明方法可以看作是对于外尔恒等式的双方的精细化. 式左的迹被更复杂的 "超迹" 所取代, 而右方则要考虑到热核的完全的渐近性态, 而这需要理解很细致的相消关系. 这种关系的最简单的例子就是**高斯–博内**(Gauss-Bonnet)**公式**

$$\chi(M) = 2\pi \int_M R,$$

这个公式把 2 维流形 M 的欧拉示性数与标量曲率联系起来了. 欧拉示性数来自于限制在 0 阶、1 阶和 2 阶外微分形式上的霍奇[VI.90]–拉普拉斯算子 $(d+d^*)^2$ 相关的热流的迹的线性组合. 一般的阿蒂亚–辛格指标定理[V.2] 的证明则用到由**狄拉克**(Dirac) **算子**的平方给出的一个算子的热流.

III.37 希尔伯特空间 (Hilbert Spaces)

向量空间[I.3 §2.3]和线性映射[I.3 §4.2] 的理论支持了很大的一部分数学. 但是, 仅用向量空间概念不能定义角的概念. 因为一般说来, 线性映射不能保持角不变. 一个内积空间可以想作具有足以使角的概念有意义的附加结构的向量空间.

内积的最简单的例子就是定义在 $\mathbf{R}^n$ 上的标准的标量积. $\mathbf{R}^n$ 就是所有长度为 n 的实数序列所成的如下的空间. 如果 $v = (v_1, \cdots, v_n)$ 和 $w = (w_1, \cdots, w_n)$ 是两个这样的序列, 它们的标量积, 记作 $\langle v, w\rangle$, 就是和 $v_1w_1 + v_2w_2 + \cdots + v_nw_n$ (例如, $(3, 2, -1)$ 和 $(1, 4, 4)$ 的标量积就是 $3\times 1 + 2\times 4 + (-1)\times 4 = 7$).

标量积的性质中有以下两点:

(i) 它对每一个变元分别为线性的, 即对任意三个向量 u, v 和 w 以及任意两个标量 λ 和 μ, 均有 $\langle \lambda u + \mu v, w\rangle = \lambda\langle u, w\rangle + \mu\langle v, w\rangle$, 以及类似于此, 有 $\langle u, \lambda v + \mu w\rangle = \lambda\langle u, v\rangle + \mu\langle u, w\rangle$.

(ii) 任意向量 v 与其自身的标量积 $\langle v, v\rangle$ 必为一个非负实数, 而当且仅当 $v=0$ 时才为 0.

在一般的向量空间中, 任意的一对元素 u 和 v 的函数 $\langle v, w\rangle$, 只要适合以上两个条件, 就称为它们的内积, 而一个具有内积的向量空间就叫做内积空间. 如果一个向量空间具有复的标量, 则对上面的 (i) 要作如下的修改.

(1′) 对任意三个向量 u, v 和 w 以及任意两个标量 λ 和 μ, 均有 $\langle\lambda u+\mu v, w\rangle=\lambda\langle u, w\rangle+\mu\langle v, w\rangle$, 以及 $\langle u, \lambda v+\mu w\rangle=\bar{\lambda}\langle u, v\rangle+\bar{\mu}\langle u, w\rangle$, 即内积对于第二个变元是共轭线性的.

这个概念之所以可以用来定义角的概念, 理由在于在 $\mathbf{R}^2$ 和 $\mathbf{R}^3$ 中, 两个向量 v 和 w 的内积, 即标准的标量积, 它的几何意义就是 v 的长度乘以 w 的长度再乘上它们的夹角的余弦. 特别是因为一个向量与自己的夹角为 0, 所以 $\langle v, v\rangle$ 就是 v 的长度的平方.

这就给了一种在内积空间里**定义**长度和角的可能性, 一个向量 v 的长度或称为其**模**, 就是 $\sqrt{\langle v, v\rangle}$, 记作 $\|v\|$. 给定两个向量 v 和 w, [由于可证明 $|\langle v, w\rangle|/\|v\|\|w\|\leqslant 1$(证明要利用上面讲的内积的性质 (ii)), 所以存在唯一的实数 $\theta, \theta\in[0, \pi]$, 使得 $\cos\theta=\langle v, w\rangle/\|v\|\|w\|$], 于是就定义这个 θ 为向量 v 和 w 的夹角. 当长度有了定义以后, 就可以谈论向量 v 和 w 的距离, 距离 $d(v, w)$ 就定义为两个向量之差的长度 $\|v-w\|$. 距离的这个定义满足*度量空间*[III.56] 的各个公理. 由于有了角的概念, 就可以说明向量 v 和 w 正交是什么意思, 简单地就是 $\langle v, w\rangle=0$.

内积空间的用处远远超出了它的说明 2 维和 3 维空间的几何学的能力, 使它真正得到认可的地方是无限维的情况. 那时, 如果它更具有附加的**完备性**, 那就更方便了, 这一点在 [III.62] 的结尾处有简短的讨论. 一个完备的内积空间就叫做**希尔伯特空间**.

下面是希尔伯特空间的两个重要例子:

(i) l_2, 这是具有标准的标量积的 $\mathbf{R}^n$ 的自然的无限维推广, 它是具有以下性质的所有实数序列 $\{a_1, a_2, a_3, \cdots\}$ 的集合, 这里要求和 $|a_1|^2+|a_2|^2+|a_3|^2+\cdots$ 收敛. $\{a_1, a_2, a_3, \cdots\}$ 和 $\{b_1, b_2, b_3, \cdots\}$ 的内积定义为 $a_1b_1+a_2b_2+a_3b_3+\cdots$(可以用*柯西–施瓦兹不等式*[V.19] 证明这个和的收敛性).

(ii) $L_2[0, 2\pi]$, 这是定义在所有实数区间 $[0, 2\pi]$ 上的满足以下条件的函数的集合: 积分 $\int_0^{2\pi}|f(x)|^2\mathrm{d}x$ 有意义而且有限. $L_2[0, 2\pi]$ 中的两个函数 f 和 g 的内积定义为 $\int_0^{2\pi}f(x)g(x)\mathrm{d}x$(由于技术性的原因, 这个定义给得不太准确, 因为现在非零的函数的范数可能为 0, 但是这个问题不难处理).

这些例子的第二个对于傅里叶分析有着中心的地位. 下面凡说到**三角函数**, 就

是指的形如 $\cos(mx)$ 或 $\sin(mx)$ 的函数. 任意两个不同的三角函数的内积为 0, 所以它们是互相正交的. 更重要的是, 三角函数起了空间 $L_2[0, 2\pi]$ 的坐标系的作用, 即这个空间的每一个函数 f 都可以表示为三角函数的 (无限) 线性组合. 这就使希尔伯特空间可以用来模拟声波, 如果函数 f 表示一个声波, 则三角函数就是纯音 (pure tone)①, 它们是声波的组成分量.

三角函数的这些性质说明了希尔伯特空间理论中的一个很重要的一般现象: 每一个希尔伯特空间都具有规范正交基底. 这就是一族具有以下三个性质的向量 e_i:

- 对于每一个 i, $\|e_i\| = 1$;
- 当 $i \neq j$ 时, $\langle e_i, e_j \rangle = 0$; 还有
- 空间中的每一个向量 v 都可以表示为收敛的和 $\sum_i \lambda_i e_i$.

三角函数还没有构成规范正交基底, 但是它们的适当的倍数却是. 除了傅里叶分析以外, 还有许多情况, 在其中, 通过把向量按照已给的正交基底分解, 会给出有用的信息, 许多一般的事实都可以由这种基底的存在导出.

希尔伯特空间 (具有复标量的) 在量子力学中也有中心的地位. 希尔伯特空间的向量表示一个量子力学系统的可能的态, 而这个系统的可观测的特性则相应于某些线性映射.

由于种种理由, 希尔伯特空间上的*线性算子*[III.50] 的研究是数学的一大分支, 详见*算子代数*[IV.15].

III.38 同调与上同调 (Homology and Cohomology)

若 X 为一*拓扑空间*[III.90], 可以对它联系上一系列群 $H_n(X, \mathbf{R})$, 其中 $\mathbf{R}$ 是一个*可换环*[III.81 §1], 如 $\mathbf{Z}$ 或 C. 这些群就是 X 的 (系数在 $\mathbf{R}$ 中的)**同调群**. 它们是强有力的不变量. 所谓强有力, 就是指它们包含了大量的关于 X 的信息, 而又容易计算, 至少是比其他不变量容易计算. 与之密切相关的**上同调群** $H^n(X, \mathbf{R})$ 甚至更加有用, 因为它们可以做成一个环, 稍微过分简单化一点地说, 上同调群 $H^n(X)$ 的元素就是余维数为 n 的子空间 Y 的*等价类*[I.2 §2.3][Y](当然, X 需要是相当 "好" 的空间, 如一个*流形*[I.3 §6.9], 才有意义). 这时, 如果取 $[Y]$ 和 $[Z]$ 分别属于 $H^n(X, \mathbf{R})$ 和 $H^m(X, \mathbf{R})$, 它们的乘积是 $[Y \cap Z]$. 因为 $Y \cap Z$ "典型地" 具有余维数 $m+n$, 所以它的等价类 $[Y \cap Z]$ 属于 $H^{m+n}(X, \mathbf{R})$. 同调群和上同调群在条目*代数拓扑*[IV.6] 中有较详细的描述.

① 所谓纯音就是具有单一频率的声波, 它具有正弦波形.—— 中译本注

同调和上同调的概念已经变得比上面的讨论所暗示的宽广得多, 而不再仅与拓扑空间相联系, 例如, 群的上同调的概念在代数学里面就有很大的重要性. 即令是在拓扑学中, 也有种种不同的同调和上同调. 1945 年, 艾伦伯格 (Eilenberg) 和 Steenrod 就设计了少数几个公理, 大大地澄清了这个领域: 一个同调理论就是把群与拓扑空间联系起来并且适合这几个公理的一种方式, 同调理论的基本性质就可以从这几个公理导出.

III.39 同 伦 群 (Hopmotopy Groups)

若 X 为一拓扑空间, X 中的**循环**就是一条起点与终点重合的路径; 或者用比较形式的说法, 循环就是一个连续函数 $f : [0, 1] \to X$, 而且 $f(0) = f(1)$. 这条路径的起点, 亦即终点, 称为**基点**. 我们说两个具有相同基点的循环是**同伦**的, 如果可以把其中的一个连续变形为另一个, 而且变形过程中所有中间的路径全在 X 中, 而且同以这个基点为起点和终点. 例如, 设 X 为平面 $\mathbf{R}^2$, 则任意始于又终于点 $(0, 0)$ 的循环都是同伦的, 而若 X 是上述平面挖去了原点, 则两个 (始于又终于另一点) 的路径是否同伦, 就要看它们是否绕过原点同样多次而定.

同伦是一个等价关系[I.2 §2.3], 以点 x 为基点的路径的等价类就构成**基本群**, 记作 $\pi_1(X, x)$. 如果 X 是连通的, 基本群就与基点 x 的选取无关, 所以就记作 $\pi_1(X)$. 这个群中的群运算就是 "连接", 给出了两个以 x 为基点的路径, 路径的 "乘积" 就是由这两个路径连接而成的路径, 即走完了一条路径接着再走完另一条路径, 路径的等价类的乘积则定义为路径乘积的等价类. 这个群是很重要的不变量 (例如可见几何和组合群论[IV.10 §7]); 它是一系列高维的同伦群的第一个, 关于这些同伦群, 请见代数拓扑[IV.6 §2, 3].

III.40 理 想 类 群 (The Ideal Class Group)

算术的基本定理[V.14]断言, 每一个正整数都可以用恰好一种方法写为素数之积 (但若把这些素数按不同次序排列, 则仍算作同一种写法). 在许多不同的背景下, 类似的定理也成立, 例如多项式就有唯一因子分解定理, 对于**高斯整数**, 即形如 $a + ib$ 而 a, b 为整数的数, 也有这样的定理.

然而对于绝大多数数域[III.63], 相关的 "整数环" 并没有唯一分解性质. 例如在形如 $a + b\sqrt{-5}$, a , b 为整数的数所成的环[III.81§1] 中, 就既可以把 6 分解为

2×3, 也可以把它分解为 $(1+\sqrt{-5})(1-\sqrt{-5})$.

理想类群就是量度唯一分解性质失的程度的一个方法. 给出一个数域的整数环, 可以在它的*理想*[III.81 §2] 的集合中定义一种乘法结构, 使得唯一分解定理对于它成立. 环自身的元素相应于所谓 "主理想", 所以如果每一个理想都是主理想, 则这个环也具有唯一分解性质. 如果还有非主理想存在, 则可以在所有理想的集合中定义一个自然的*等价关系*[I.2 §2.3] 使得这些等价类 (称为**理想类**) 构成一个*群*[I.3 §2.1], 这个群就是**理想类群**. 所有的主理想都属于这个群的恒等元这个等价类. 所以理想类群越大越复杂, 这个环就离唯一分解性质越远. 更多的细节可见条目*代数数*[IV.1], 特别是其中的 §7.

III.41 无理数和超越数

(Irrational and Trancendental Numbers)

Ben Green

一个无理数就是一个不能写为 a/b 而 a 和 b 均为整数的数. 有许多自然出现的无理数, 例如 $\sqrt{2}$,e 和 π. 下面关于 $\sqrt{2}$ 为无理数的证明可能是整个数学中最广为人知的证明. 如果 $\sqrt{2}=a/b$, 因为公因子可以约去, 可以假设 a 和 b 没有公因子. 这样, 就会有 $a^2=2b^2$, 这意味着 a 必须为偶数; 把 a 写成 $2c$, 这时又会得到 $4c^2=2b^2$, 所以 $2c^2=b^2$, 这又意味着 b 也必定为偶数, 这就与假设 a 和 b 为互素矛盾.

关于某个特定的数是有理数还是无理数, 在数学中有几个有名的猜想. 例如, 迄今仍然不知道 $\pi+\mathrm{e}$ 和 π^{e} 是否无理数, 也不知道, 欧拉常数

$$\gamma=\lim_{n\to\infty}\left(1+\frac{1}{2}+\cdots+\frac{1}{n}-\log n\right)\approx 0.577215\cdots$$

是否无理数. 已经知道 $\zeta(3)=1+2^{-3}+3^{-3}+\cdots$ 是一个无理数. 几乎可以断定 $\zeta(5),\ \zeta(7),\ \zeta(9),\cdots$ 都是无理数. 然而, 虽然可以证明这些数中有无限多个都是无理数, 但是不知道其中某一个确定的数是无理数.

e 的无理性的证明是经典的. 若

$$\mathrm{e}=\sum_{j=1}^{\infty}\frac{1}{j!}$$

是一个有理数 p/q, 就会有

$$p(q-1)!=\sum_{j=0}^{\infty}\frac{q!}{j!}.$$

式左和式右的前几项, 即 $j \leqslant q$ 的项都是整数, 所以,

$$\sum_{j\geqslant q+1}\frac{q!}{j!}=\frac{1}{q+1}+\frac{1}{(q+1)(q+2)}+\cdots$$

也是一个整数, 但是不难证明右方的量严格地位于 0 和 1 之间, 这就是一个矛盾.

这里用到的原理, 即一个整数的绝对值至少是 1. 这是一个简单的事实, 但是在无理数和超越数理论中, 却是惊人地强有力.

有一些数比其他数更加 "无理". 在某种意义下, 黄金分割比 $\tau=\frac{1}{2}(1+\sqrt{5})\approx 1.618$ 是最无理的[①], 意思是说它的有理近似, 即斐波那契数列相继的项的比收敛于它极为缓慢. 关于 τ 的无理性, 有一个美妙的证明. 这个证明是基于下面的事实: 作一个 $\tau\times 1$ 矩形 R, 它可以分解成一个边长为 1 的正方形和一个 $1/\tau\times 1$ 的矩形之并. 如果 τ 是一个有理数, 我们就可以作出一个边长为整数的矩形与 R 相似. 从这个矩形中我们可以去除一个正方形, 使得余下一个边长仍为整数的矩形, 而且仍然与 R 相似. 可以无限地这样作下去, 但这显然是不可能的.

超越数就是一个非**代数数的实数**, 就是说, 不是一个具有整系数的多项式的实根. 这样 $\sqrt{2}$ 就不是一个超越数, 因为它是多项式方程 $x^2-2=0$ 的根. 同样 $\sqrt{7+\sqrt{17}}$ 也不是超越数.

是否真有超越数存在? 刘维尔[VI.39] 在 1844 年回答了这个问题, 他证明了有好几个数都是超越数, 其中一个著名的例子是

$$\kappa=\sum_{n\geqslant 1}10^{-n!}=0.110001000000000000000001000\cdots,$$

它不是代数数, 因为它可以用有理数来逼近, 其精度不是任何代数数所容许的. 这句话的意思是, 虽然 110 001/1 000 000 是一个很接近于 κ 的有理数, 但是它的分母不够大.

刘维尔证明了若 α 是一个 [具有整系数的]n 次多项式方程的根, 则存在一个依赖于 α 的常数 C, 使得对于所有的整数 a 和 q 都有

$$\left|\alpha-\frac{a}{q}\right|>\frac{C}{q^n}.$$

用口头语言来说, 即代数数不可能用有理数逼近得太好. 后来罗特[②] 把这里的 n 改进为 $2+\varepsilon$, $\varepsilon>0$ 是任意正数 (关于这个问题, 更多的内容可见条目刘维尔定理和罗特定理[V.22]).

① 见欧几里得算法和连分数[III.22 §2], 特别是式 (9).—— 中译本注

② 就是 Klaus Friedrich Roth, 1925 年生于德国, 年轻时就来到英国. 他在 1955 年证明了这里说的定理, 而于 1958 年得到 Fields 奖.—— 中译本注

30 年后, 康托[VI.54] 用完全不同的方法又发现了超越数的存在, 他证明了代数数的集合是可数的[III.11], 粗略地说, 就是代数数可以按次序列成一个清单. 精确地说, 就是存在一个由自然数的集合 $\mathbf{N}$ 到代数数集合的一个满射. 与之相对照, 实数集合 $\mathbf{R}$ 则是不可数的. 关于这个问题, 康托的著名证明, 用对角线论证来证明不论用什么样的方法来列出实数的清单, 必定是有遗漏的. 所以, 一定存在不是代数数的实数.

想要证明一个特定的数是超越数, 一般说来是很难的事. 例如, 绝不是超越数都能用有理数作很好的逼近. 能用有理数作很好的逼近, 只是一个数为超越数的充分条件, 还有其他的确定一个数为超越数的方法. e 和 π 都已经知道是超越数, 而且也知道对于一切 $\varepsilon > 0$ 有 $|\mathrm{e} - a/b| > C(\varepsilon)/b^{2+\varepsilon}$, 所以 e 并不能用有理数逼近得那么好. 因为 $\varsigma(2m)$ 总是 π^m 的有理倍数, 所以 $\varsigma(2), \varsigma(4), \cdots$ 都是超越数.

现代的超越数理论里面有许多漂亮的结果. 一个早期的结果是盖尔范德 - Schneider 定理, 它指出, 如果 $\alpha \neq 0$, 1 是一个代数数, 而 β 是一个代数数而非有理数, 则 α^β 是一个超越数. 特别是, $\sqrt{2}^{\sqrt{2}}$ 是一个超越数. 还有一个**六指数定理**: 如果 x_1, x_2 是两个线性无关的复数, 而 y_1, y_2, y_3 是三个线性无关的复数, 则以下六个数

$$\mathrm{e}^{x_1y_1}, \mathrm{e}^{x_1y_2}, \mathrm{e}^{x_1y_3}, \mathrm{e}^{x_2y_1}, \mathrm{e}^{x_2y_2}, \mathrm{e}^{x_2y_3}$$

中, 至少有一个是超越数. 与此相关的还有 (至今仍未解决的)**四指数猜想**: 若 x_1, x_2 是两个线性无关的复数, 而 y_1, y_2 也是线性无关的 [复数], 则下面四个数

$$\mathrm{e}^{x_1y_1}, \mathrm{e}^{x_1y_2}, \mathrm{e}^{x_2y_1}, \mathrm{e}^{x_2y_2}$$

中, 至少有一个是超越数.

III.42　伊 辛 模 型 (The Ising Model)

伊辛 (Ernst Ising, 1900–1998, 德国物理学家) 模型是统计物理的基本模型之一. 它的设计原来是为了说明铁磁物质在加热时的性态, 但是后来又被用于许多其他现象的模型.

下面是这个模型的一个特例. 令 G_n 为所有绝对值最多为 n 的整数的对子的集合. 所谓 G_n 的**构型**(configuration), 就是对 G_n 中的每一点 x 指定一个数 σ_x 的方法, 这里的 σ_x 等于 $+1$ 或 -1. 点代表原子, 而 σ_x 则表示这个原子是 “自旋向上” 或 “自旋向下”. 相对于每一个构型 σ, 都可以附加上一个能量 $E(\sigma) = -\sum \sigma_x\sigma_y$, 这里是对所有相邻的点的对子 x, y 来求和. 这样, 当许多点都与其某些相邻的

点符号不同时, 能量就很大, 而当 G_n 可以分成两大团具有相同符号的点时, 能量就小.

每一个构型各有一个正比于 $\mathrm{e}^{-E(\sigma)/T}$ 的概率. 这里 T 是一个正实数, 表示温度, 所以能量小的构型概率就大. 这样, 构型就有一种具有同符号的点成团的趋势. 但是, 当温度增加时, 这种成团的效应就会变小, 因为各种构型的概率这时会倾向于相等.

具有零位能的 2 维伊辛模型就是这个模型当 n 趋向无穷时的极限. 关于更一般的模型和与此相关的相变的讨论, 可见条目临界现象的概率模型[IV.25 §5].

III.43 约当法式 (Jordan Normal Form)

假设给了一个实的或复的 $n \times n$ 矩阵[I.3 §4.2] A, 若想要理解它. 则可以探求它作为 $\mathbf{R}^n$ 或 $\mathbf{C}^n$ 上的线性映射[I.3 §4.2] 有何性态, 也可能想知道 A 的幂是什么. 一般地, 回答这些问题并不那么容易. 但是对于某些矩阵却是很容易的. 例如, 若 A 是一个**对角矩阵**(就是所有非零元素全在**主对角线上**的矩阵), 这两个问题都立即可以回答: 令 x 为 $\mathbf{R}^n$ 或 $\mathbf{C}^n$ 中的向量, 则 Ax 是这样的向量, 只要把向量 x 的各个分量乘以主对角线上相应的矩阵元素即可. 想要得到 A^m, 只要把主对角线上的各个元素都乘 m 次方即可.

所以, 给定了一个线性映射 T(由 $\mathbf{R}^n$ 到 $\mathbf{R}^n$ 或由 $\mathbf{C}^n$ 到 $\mathbf{C}^n$), 如果能够找到一个基底, 使得 T 对于这个基底成为一个对角矩阵, 那将是很好的, 如果能做到这一点, 就说是"了解"这个线性映射了. 说这样一个基底存在, 就相当于说存在一个全由本征向量[I.3 §4.3] 构成的基底, 如果有这样一个基底存在, 就说这个线性映射是**可对角化**的. 当然也可以把这些名词用于一个矩阵 (因为矩阵 A 通过把 x 映为 Ax, 定义了一个 $\mathbf{R}^n$ 或 $\mathbf{C}^n$ 上的线性映射), 所以当这样一个由本征向量构成的基底存在时, 也说这个矩阵是可对角化的, 这也等价于说存在一个可逆矩阵 P, 使得 $P^{-1}AP$ 是对角矩阵.

是否每一个矩阵都可以对角化? 在实数域上, 由于不足道的理由, 答案是否定的, 因为可能根本就没有 [实的] 本征向量. 所以要限制在复数域上的矩阵和线性映射.

如果有一个矩阵 A, 则由代数的基本定理[V.13], 其特征多项式, 即 $\det(A-\lambda I) = 0$, 必定有根. 令 λ 是这样一个根, 线性代数的标准事实告诉我们, $A-\lambda I$ 是奇异的, 所以存在一个 [非零] 向量 x 使 $(A-\lambda I)x=0$, 也就是 $Ax=\lambda x$. 这样, 就至少有了一个本征向量. 然而很不幸, 不一定存在足够构成一个基底的那么多本征向

量. 例如, 考虑映 $(1, 0)$[①] 到 $(0, 1)$ 而映 $(0, 1)$ 到 $(0, 0)$ 的线性映射 T. 它对于显然的基底的矩阵是 $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$, 这个矩阵就不可能对角化. 要明白这是为什么, 有一个方法如下: 这个映射 T 的特征多项式 [(就是相应矩阵的特征多项式)] 是 t^2, 它只有唯一的根 0. 经简单的计算就可以看到, 若 $Ax = 0$, 则 x 必定是 $(0, 1)$ 的倍数, 所以找不到两个线性无关的本征向量. 一个更漂亮的证明方法是注意到 $T^2 = 0$(它把 $(1, 0)$ 和 $(0, 1)$ 都映为 $(0, 0)$), 所以, 如果 T 是可对角化的, 则主对角线上的元素一定全为 0(因为非零对角矩阵的平方必为非零的), 所以 T 必须为零矩阵, 而如上面讲的, 它不是零矩阵.

用类似的论据可以证明, 若对 [某个正整数]k 有 $A^k = 0$, 则除非 A 是零矩阵, 则一定不可能对角化. 这种矩阵 A 称为**幂零矩阵**. 这一点对于所有非零元素全在主对角线下方的矩阵当然也是适用的, [因为不难证明这种矩阵必定是幂零矩阵].

那么, 对于上面这种不能对角化的矩阵 T, 又有什么可以说的呢? 我们在某种意义下感觉到, $(1, 0)$ 也 "近乎" 就是一个本征向量, [因为现在本征值 $\lambda = 0$, 所以本征向量 x 应该满足 $Tx = 0$, 但是并没有 $T(1, 0) = 0$, 而是]$T^2(1, 0) = 0$. 如果想要扩充我们的观点, 把这种向量也考虑进来, 又会发生什么事情呢? 我们将会说, 如果对于本征值 λ, 使 $T - \lambda$ 的某个幂把 x 映为 0, 则 x 是相应于这个本征值的**广义本征向量**. 在上面的例子中, $(1, 0)$ 就是相应于本征值 0 的广义本征向量. 正如对于每一个本征值都有一个 "本征空间"(即相应于本征值 λ 的本征向量所称的空间) 一样, 也有一个 "广义本征空间", 由对应于本征值 λ 的广义本征向量构成.

把一个矩阵对角化, 相当于把向量空间 (现在是 $\mathbf{C}^n$) 分解为本征空间. 所以现在自然希望, 对于任意的矩阵, 能够把向量空间分解为这个矩阵的广义本征空间. 结果这确实是可能的. 这时, 矩阵就会取**约当法式**, 下面就来比较详细地讲这件事.

现在把这件事暂时放在一边, 而来问什么是得到广义本征空间的最简单的情况? 那肯定就是把上面的例子推广到 n 维. 换句话说, 有一个线性映射 T, 它把 e_1 映为 e_2, 把 e_2 映为 e_3, 这样下去直到把 e_{n-1} 映为 e_n, 但是把 e_n 映为 0. 这个映射就是

$$\begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & 0 \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{pmatrix}.$$

这个矩阵虽然不能对角化, 但是至少是很容易懂的.

① 本条目下面时常把竖列向量写成横行向量. —— 中译本注

一个矩阵的约当法式就是这一类矩阵的对角和, 只要看到上面的矩阵就是这类矩阵之一, 这类矩阵就很容易懂了. 当然, 我们要考虑不是零的本征值, 所以定义以下形状的矩阵为一个约当方块:

$$\begin{pmatrix} \lambda & 0 & 0 & \cdots & 0 & 0 \\ 1 & \lambda & 0 & \cdots & 0 & 0 \\ 0 & 1 & \lambda & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & \lambda \end{pmatrix}.$$

注意, 从这个矩阵 A 减去 λI 就是上面的那个矩阵, 所以 $(A-\lambda I)^n$ 确实就是零矩阵. 所以, 一个约当方块表示一个确实容易懂的线性映射, 而所有的 [满足方程 $(A-\lambda I)^n x=0$ 的] 向量 x, 就是相应于同一个本征值 λ 的广义本征向量. 约当法式定理告诉我们, 每一个矩阵都可以分解为这种约当方块, 就是说一个矩阵如果具有以下形状, 那就是其约当法式,

$$\begin{pmatrix} B_1 & 0 & \cdots & 0 \\ 0 & B_2 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & B_k \end{pmatrix}.$$

这里的 B_i 都是约当方块, 但是大小不同, 这里的 0 都是一些以 0 为元素的矩阵, [其行数等于其右方的约当方块的行数, 其列数则等于其上方的约当方块的列数]. 一个大小为 1 的约当方块就是一个本征值①.

一个矩阵 A 化成了约当法式, 也就是空间分解成了一些子空间, 而在每一个子空间上, A 的作用就容易理解了. 例如, 设 A 是下面的矩阵:

$$\begin{pmatrix} 4 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 4 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 4 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 4 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 4 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 2 \end{pmatrix}.$$

它由 3 个约当方块构成, 其大小分别是 3, 2, 2, 然后就立刻可以从这里读出大量关于 A 的信息. 例如考虑本征值 4, 它的代数重数 (即作为特征多项式的根的重数)

① 原书说是本征向量, 是一个误排. —— 中译本注

是 5, 这是所有以 4 为本征值的约当方块**大小**的和; 而它的几何重数 (即相应的由本征向量构成的本征空间的维数) 是 2, 这是以 4 为本征值的约当方块的**个数**(因为每一个约当方块只含有 1 个真正的本征向量, [其余的是广义本征向量]), 甚至矩阵的最小多项式 (就是次数最低的使得 $P(A)=0$ 的多项式 $P(t)$) 也容易写出来. 每一个约当方块的最小多项式可以立刻写出来：若这个约当方块的大小是 k 而本征值[①] 为 λ, 则这个约当方块的最小多项式就是 $(t-\lambda)^k$. 而整个矩阵的最小多项式就是各个约当方块的最小多项式的 "最低公倍". 对于上面的矩阵, 会得到各个约当方块的最小多项式分别是 $(t-4)^3$, $(t-4)^2$ 和 $(t-2)^2$, 所以全矩阵的最小多项式应该是 $(t-4)^3(t-2)^2$.

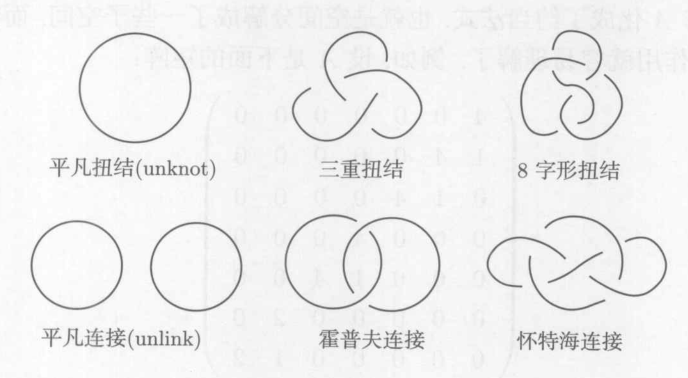
约当法式在作用于向量空间的线性映射的背景之外, 还有一些推广. 例如, 有一个适用于阿贝尔群的类似的定理, 就是每一个有限阿贝尔群都可以分解为循环群的直积.

III.44 纽结多项式 (Knot Polynomials)

W. B. R. Lickorish

1. 扭结与连接

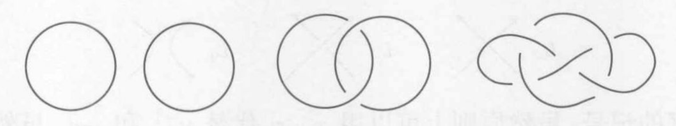
一个**扭结**就是一条在 3 维空间中首尾相连但是不自交的曲线. 一个**连接**就是几条这样的互相分离的曲线, 而每一条曲线就叫做这个连接的分支. 下面是一些简单的例子：



如果两个扭结中的一个能够连续地变形为另一个, 而在此过程中不弄断 "弦

① 原书误为广义本征值, 只有广义本征向量, 而没有广义本征值一说.—— 中译本注

线", 就说它们是等价的, 即 "相同的". 这个变形过程有一个专门名词, 叫做**同痕**(isotopy), 例如, 下面 3 个扭结都是 "相同的", 即互相同痕:



扭结理论的第一个问题, 就是如何决定两个扭结是否相同. 两个扭结可能看起来很不相同, 但是怎么证明它们其实是相同的? 在经典的几何学里, 两个三角形如果能够刚性地把一个移动为另一个, 就说它们是相同的 (或全等的). 对于每一个三角形的各个边与角都指定一个量度边长或角度的数, 以便用这些数来决定它们是否全等. 类似地, 对于扭结和连接, 也有一些与它们相连的数学实体称为**不变量**, 而如果两个连接有不同的不变量, 它们就不可能是相同的. 许多不变量是与一个连接在 3 维空间中的余集合的几何与拓扑有关的. 这个余集合的*基本群*[IV.6 §2] 就是一个出色的不变量, 但是这就需要一些代数技巧来区别开这些基本群. 亚历山大 (J. W. Alexander) 多项式 (1926 年发表) 就是从区别这些基本群而导出的连接的不变量. 亚历山大多项式虽然来源是*代数拓扑*[IV.6], 却很早就知道它们满足一种 "束关系"(skein relation)(见下文). 1984 年提出的 HOMFLY① 多项式, 推广了亚历山大多项式, 但是只与束理论的简单的组合学有关.

1.1 HOMFLY 多项式

设一个连接是有定向的, 所以其每一个分支都有方向, 用箭头表示. 对于每一个有向连接 L 都可以指定它的 HOMFLY 多项式 $P(L)$, 这是一个含 2 变量 v 和 z 的多项式 (但其中允许有 v 和 z 的正负整数幂). 这些多项式是这样的: 首先

$$P(\text{平凡扭结}) = 1, \tag{1}$$

其次, 有一个线性的**束关系**

$$v^{-1}P(L_+) - vP(L_-) = zP(L_0), \tag{2}$$

这里的 L_+, L_- 和 L_0 分别是下面图式的连接或扭结 (L_0 即平凡扭结). L_+ 的实线 (由西南指向东北, 称为上行桥 (over-pass), 另一条中间断了的称为下行桥 (under-pass); L_- 的意思类似. [这些名词都是从立交通道的术语借来的]; L_0 则是不连接, 所以是平凡连接, 也可以说是平凡扭结]. (2) 式的意思是如果有 3 个连接, 它们

① HOMFLY 是由这个理论的共同发现者 Hoste, Ocneanu, Millet, Freyd, Lickorish, Yetter 的姓的第一个字母合成的, 有时还加上另两位独立的发现者 Prztycki 和 Traczyk 成为 HOMFLY-PT. "束关系" 的 "束", 英文是 skein, 原意是一团羊毛或一束纱线, 用于扭结和连接的理论是很形象的.—— 中译本注

除了在交叉点附近可以取上面 3 种形式之一外, 其他地方都是相同的, 则它们的 HOMFLY 多项式必定满足 (2) 式.

L_+ L_- L_0

这是很好的记号, 虽然原则上可以用 x , y 代替 v^{-1} 和 $-v$. 虽然亚历山大多项式已经满足 (2) 的一个个例, 但是等待了 60 年以及琼斯 (Jones) 的多项式的发现, 人们才认识到, 可以利用 (2) 这样一般的线性关系. 注意, 在连接的图式上, 相交有两种类型. 一个相交称为是**正的**, 如果沿下行桥按照箭头方向接近交叉点, 会看到另一条有向的弧线 (即上行桥) 是由左到右的, [即图上的 L_+]; 如果上行桥是从右到左, [如图上的 L_-], 则说这个相交是**负的**. 当在一个连接的交叉点处解释束关系时, 则若交叉为正, 就要把 L 看成 L_+, 为负是看成 L_-, 这是至关重要的.

支撑这个理论的定理就是, 对于有向的连接, 可以用一种协调的方式唯一地指定一个多项式, 而与如何选择这个连接的图式无关. 这个定理远非显然自明的. 可以在 Lickorish(1997) 中找到证明.

1.2 HOMFLY 计算

在扭结的图式中, 总可以通过把某个交叉点的上行桥换成下行桥或相反而得出一个平凡扭结, 连接也可以这样类似地解开. 由这一点就可以利用上面给的等式来计算出多项式, 虽然计算的长度对于交叉点的个数是指数增长的. 下面就是 P(三重扭结) 的计算, 首先考虑束关系的以下个例:

$$v^{-1}P(\;)-vP(\;)=zP(\;)$$

把两个平凡扭结的多项式换成多项式 1, 就说明这个两个分支的连接的 HOMFLY 多项式是 $z^{-1}\left(v^{-1}-v\right)$. 使用束关系的第二个例子是

$$v^{-1}P\left(\;\right)-vP\left(\;\right)=zP\left(\;\right).$$

把前面关于平凡连接的答案代入, 就得到霍普夫 (Hopf) 连接的 HOMFLY 多项式是 $z^{-1}(z^{-3}-v^{-1})-zv^{-1}$. 最后, 再看束关系的下面的个例:

$$v^{-1}P\left(\;\right)-vP\left(\;\right)=zP\left(\;\right).$$

把前面计算出的霍普夫连接的多项式, 以及平凡扭结的多项式 1 都代入, 说明

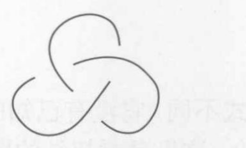
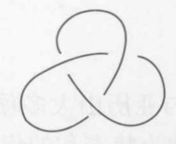
$$P(\text{三重扭结})=-v^{-4}+2v^{-2}+z^2v^{-2},$$

类似的计算又可给出

$$P(8\text{ 字形扭结}) = v^2 - 1 + v^{-2} - z^2 .$$

三重扭结和 8 字形扭结的多项式是不同的, 这就证明了它们是不同的扭结. 做一个实验, 用一条项链做一个三重扭结 (用项链头上的钩子把它的两端连起来) 就会发现, 确实不可能把它变成一个 8 字形扭结. 还要注意, 一个扭结的多项式不依赖于其上定向的选择 (但是一个连接则不然).

一个扭结在镜子里的反射等价于在扭结的图式中每一个交叉点处的上行桥变成下行桥以及相反 (把这个图式所在的平面就看成一面镜子). 反射后的扭结处处都与原扭结一样,

除了 v 的每一次出现都要换成 $-v^{-1}$. 这样, 三重扭结和它的反射像的多项式分别为

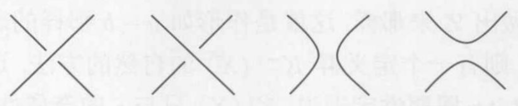
$$-v^{-4} + 2v^{-2} + z^2v^{-2}\text{和} - v^4 + 2v^2 + z^2v^2 .$$

因为这些多项式不同, 所以三重扭结和它的反射是不同的扭结.

2. 其他的多项式不变量

HOMFLY 多项式的发现是受到了 1984 年琼斯所发现的多项式的启发. 对于有向连接 L, 琼斯多项式 $V(L)$ 只含一个变量 t(还有 t^{-1}), 它是在 $P(L)$ 中令 $v = t$, $z = t^{1/2} - t^{-1/2}$ 而得出的, 这里的 $t^{1/2}$ 是 t 的一个形式平方根. 亚历山大多项式则是由令 $v = 1$, $z = t^{-1/2} - t^{1/2}$ 而得出的. 这种多项式可以用拓扑学中的基本群、覆迭空间和同调理论来很好地理解, 可以用涉及行列式的各种方法来计算. 第一个发展了束关系理论的则是康韦 (J. H. Conway), 他在 1969 年讨论他的亚历山大多项式 (这是在 HOMFLY 多项式中令 $v = 1$ 而得的一个变量 z 的多项式) 的规范化版本时发展了这个理论.

还有一种基于一个线性束关系的多项式 (归功于 L. H. Kauffman). 这个束关系涉及 4 个具有无定向图式的不同的连接如下:



有这样的例子, 就是有一对扭结是 Kauffman 多项式可以区别, 而 HOMFLY 多项式则不能区别, 或者相反; 还有一些对扭结, 两种多项式都不能加以区别.

2.1 对交错扭结的应用

对于琼斯多项式有一种特别简单的使用 “Kauffman 括弧多项式” 的陈述, 使我们能容易地证明琼斯多项式可以无矛盾地定义 (但不能用于 HOMFLY 多项式). 这个途径被用来给出 P.G. Tait (1898) 的一个高度可信的建议的第一个严格的证明, 这个建议是说, 一个扭结的简化了的交错图式, 在此扭结的所有图式中, 给出了交叉点最少的图式. 这里所谓 “交错” 是指沿着扭结的图式, 交叉点依次是 $\cdots$ 上、下、上、下、上 $\cdots$. 并非所有的扭结都有这样的图式. 所谓 “简化” 是说, 图式的平面余集合有 4 个不同的区域邻接着每一个交叉点. 这样, 例如任意的非平凡的简化的交错图式都不是平凡扭结的图式. 还有 8 字形扭结, 肯定没有只有 3 个交叉点的图式.

2.2 物理

HOMFLY 多项式与亚历山大多项式不同, 它没有已知的用经典的代数拓扑的解释. 但是, 它可以陈述为状态和的集合, 这里是对扭结的图式的某些标号来求和. 这就令人想起来自统计物理学的思想: 在 Kauffman(1991) 中有初等的讲解. 整个 HOMFLY 多项式理论的放大, 引导到共形场论的一个版本, 称为拓扑量子场论.

进一步阅读的文献

Kauffman I H. 1991. *Knots and Physics.* Singapore: World Scientific.

Lickorish W B R. 1997. *An Introduction to Knot Theory.* Graduate Texts in Mathematics, volume 175. New York: Springer.

Tait P G. 1898. On Knots. In *Scientific Papers*, volume 1, 237-347. Cambridge: Cambridge University Press.

III.45 K 理 论

(K-Theory)

K 理论讲的是**拓扑空间**[III.90]X 的最重要的不变量之一, 这是一对群, 称为 X 的 K 群. 为了构造出群 $K^0(X)$, 取 X 上的所有向量丛 (的等价类), 并以直和为群运算. 这并没有引导到一个群, 而是引导到一个半群. 然而, 从半群可以做出一个群来, 正如可以从 $\mathbf{N}$ 做出 $\mathbf{Z}$ 来那样, 这就是作形如 $a-b$ 那样的表达式的等价类. 如果 i 是一个正整数, 则有一个定义群 $K^{-i}(X)$ 的自然的方法, 这与群 $K^0(S^i\times X)$ 密切相关. 重要的 **Bott 周期性定理**说, $K^i(X)$ 只与 i 的奇偶性相关, 所以, 事实上只有两个不同的 K 群, 即 $K^0(X)$ 和 $K^1(X)$. 详见**代数拓扑**[IV.15§4.4].

如果 X 是一个拓扑空间如紧流形, 则可以附加上一个由 X 到 $\mathbf{C}$ 的连续函数

所成的 C^*- 代数 $C(X)$. 于是可以用这个代数来定义 K 群, 使它可以用于不是形如 $C(X)$ 的代数, 特别是可以用于乘法不可交换的代数. 例如, K 理论提供了 C^*-代数的重要的不变量, 见算子代数[IV.15§4.4].

拉格朗日乘子
(Lagrange Multipliers)

见优化与拉格朗日乘子 [III.64]

III.46 利奇格网
(The Leech Lattice)

为了定义 $\mathbf{R}^d$ 中的格网, 取 d 个线性无关的向量 $v_1, \cdots, v_d$, 并且作出所有形如 $a_1v_1 + \cdots + a_dv_d$ 的线性组合, 其中 $a_1, \cdots, a_d$ 是整数. 例如, 想要定义 $\mathbf{R}^2$ 中的一个六边形格网, 可以取 v_1, v_2 分别为 $(1, 0)$, $\left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$. 注意, v_2 可以由v_1 旋转 $\pi/3$ 而得, $v_2 - v_1$ 可以由 v_2 旋转 $\pi/3$ 而得. 这样旋转下去, 就可以得出绕原点的正六边形的所有顶点.

正六边形格网在所有的 $\mathbf{R}^2$ 格网中是不寻常的, 即它有 6 阶的旋转对称性, 这使它在许多方面成为 "最佳" 的格网 (例如, 蜜蜂就把蜂巢安排成六边形格网, 一团大小相仿的肥皂泡也自然地组织成为六边形格网, 等等). 利奇 (John Leech, 1926–1992, 英国数学家) 格网在 24 维空间中也起类似作用, 在 24 维格网中, 它是 "最对称" 的, 其对称的程度非常异乎寻常. 在条目数学研究的一般目的[I.4 §4] 中有比较详细的讨论.

III.47 L 函 数
(L-Functions)

Kevin Buzzard

1. 怎样把一个数列 "打包"

设有一个数列, 例如

$$\pi, \sqrt{2}, 6.023 \times 10^{23}, \cdots,$$

怎样把它打包成为一个对象, 而且使它能够记住关于这个数列的一切, 甚至可能给我们关于这个数列的新的洞察? 一个标准的技巧是使用生成函数[III.32], 但是还有一个方法, 已经证明在数论和在别处都富有成果. 给定了一个数列 $a_1, a_2, \cdots$, 可以定义**狄利克雷级数**

$$L(s) = \frac{a_1}{1^s} + \frac{a_2}{2^s} + \frac{a_3}{3^s} + \cdots = \sum_{n\geqslant 1} a_n/n^s,$$

这里的 s 既可以是正整数, 也可以是例如实数. 只要 $a_1, a_2, \cdots$ 增长不是太快 (以下都这样假设), 级数 $L(s)$ 对于实部充分大的值 s 总是收敛的. 进一步说, 哪怕初始的序列很简单, 它也可能是一个非常 "丰富" 的对象. 例如, 设对所有的 n, $a_n = 1$, 这样得到的 $L(s)$ 就是著名的黎曼 ς 函数[IV.2§3]: $\varsigma(s) = 1^{-s} + 2^{-s} + 3^{-s} + \cdots$, 当 $s > 1$ 时, 它是收敛的, 而且欧拉证明了它满足以下的等式 (其中包含了对于某些偶数 s 的 $\varsigma(s)$ 之值):

$$\varsigma(2) = \pi^2/6, \quad \varsigma(4) = \pi^4/90, \quad \varsigma(12) = \frac{691\pi^{12}}{638\,512\,875}.$$

这样, 甚至对于简单如 $1, 1, 1, \cdots$ 这样的序列, 也提出了一些自然的迫切需要解决的问题.

ς 函数是 L 函数的原型的例子. 但是, 并不是每一个狄利克雷级数都值得称为 L 函数. 下面举出 ς 函数的一些 "好" 的性质. 粗略地说, 如果一个狄利克雷级数具有这些性质, 就说它是一个 L 函数, 这当然不算是一个正式的定义. 但是, 事实上并没有 "一个 L 函数" 的所谓正式的定义 (人们曾经试图给出一个这样的定义, 但是, 哪一个才算是正确的定义, 对此并无共识). 实际情况是, 如果一个数学家找到的一个方法, 使得数列 $a_1, a_2, \cdots$ 与一个数学对象 X 有了联系, 而又有证据表明相应的狄利克雷级数 $L(s)$ 具有 ς 函数的好性质, 这时就说 $L(s)$ 是 X 的 L 函数.

2. $L(s)$ 可能有什么好性质

可以验证, ς 函数可以表示成为一个无穷乘积 $\prod_p (1-p^{-s})^{-1}$, 这里的 p 是一切素数. 这个乘积常称为**欧拉乘积**, 而一个狄利克雷级数如果当得起 L 函数这个头衔, 它就应该也有类似的乘积展开式. 这种展开式的存在与序列 $a_1, a_2, \cdots$ 具有**乘法性质**(multiplicative) 密切相关但又稍强, 乘法性质就是: 当 a_m, a_n 互素时, $a_{mn} = a_m a_n$.

为了前进一步, 需要扩大我们的视野. 不难证明 $L(s)$ 的定义当 s 为 1 时也是有意义的, 只要 s 具有充分大的实部即可. 此外, 它在使得这个和收敛的复平面区域上定义一个全纯函数[I.3§5.6]. 例如, 定义 ς 函数的狄利克雷级数对于每一个适

合 $\mathrm{Re}(s)>1$ 的 s 都是收敛的. 关于 ς 函数的一个标准的事实就是, 它可以唯一地拓展为对于一切 s, $\mathrm{Re}(s)\neq 1$ 的全纯函数. 这个现象称为 ς 函数的**亚纯拓展**. 这一点类似于无穷和 $1+x+x^2+x^3+\cdots$ 只在 $|x|<1$ 时收敛, 但若写成 $1/(1-x)$ 则对于任意不等于 1 的复数 x 都有意义. 具有亚纯拓展是我们期望于一般的 L 函数的一个性质. 然而, 对于随机的序列 a_1, a_2, a_3, $\cdots$, 把相应的狄利克雷级数拓展为整个复平面上的函数, 并不是一个 "纯粹形式的" 手段. 对于它, 完全没有理由要求相关的狄利克雷级数 $L(s)$ 能够拓展到这个级数的收敛区域之外. 亚纯拓展的存在在某种意义上是断定存在某种更微妙的对称性的严格的说法.

关于亚纯拓展, 应该简要地提一下黎曼假设[V.26], 这是一个猜想, 说如果把 $\varsigma(s)$ 拓展为整个复平面上的全纯函数, 则 $\varsigma(s)$ 的零点[①], 即使得 $\varsigma(s)=0$ 的点, 必定都具有实部 $\frac{1}{2}$, 即位于直线 $\mathrm{Re}(s)=\frac{1}{2}$ 上. 对于许多 L 函数也都有类似的黎曼假设, 而几乎所有的都是未解决的问题.

我们需要强调的最后一个性质是在 $\varsigma(s)$ 和 $\varsigma(1-s)$ 之间有比较简单的关系式. 这些关系式称为 ς 函数的**函数方程**, 而任何称得起 L 函数这个名称的狄利克雷级数也应该有这个性质 (一般地会去寻求 $\bar{L}(s)$ 和 $\bar{L}(k-s)$ 之间的关系式, 其中 k 是一个实数, 而 $\bar{L}(s)$ 是相应于复共轭序列 $\bar{a}_1$, $\bar{a}_2$, $\bar{a}_3$, $\cdots$ 的狄利克雷级数).

在数论里面有许多狄利克雷级数的例子, 它们具有或者猜想具有这三个关键的性质: 一个欧拉乘积、具有亚纯拓展和一个函数方程. 这些狄利克雷级数后来就被称为 L 函数. 例如, 设 A, B 是两个整数, 使得三次方程

$$y^2=x^3+Ax+B \tag{1}$$

的 3 个根都是单根, (1) 定义了一条椭圆曲线[III.21], 与之相关有一个序列 $a_1, a_2, \cdots$ (其中 a_n 与 (1) 的根的个数 mod n 相关, 至少当 n 为素数时如此, 详见算术几何[IV.5 §5.1]). 然而确定与它相关的狄利克雷级数在复平面上的亚纯拓展 $L(s)$ 是一个多年没有解决的问题. 现在由于怀尔斯 · 泰勒等人关于费马大定理[V.10] 的工作, 已经知道这个亚纯拓展是存在的 (而且没有极点).

3. L 函数的要点何在

L 函数的最早的应用之一是由狄利克雷[VI.36] 本人给出的, 狄利克雷用它来证明在一般的算术序列中必有无穷多个素数存在 (见解析数论[IV.2 §4]). 事实上, 虽然黎曼假设还未得到证明, 甚至关于黎曼 ς 函数的零点的位置的部分结果在素数分布理论上也有深刻的推论.

然而, 近百年来数学家已经找到它们的第二个用途: 若 X 是一个数学对象, 而 $L(s)$ 是相应的 L 函数, 关于 X 的算术与 $L(s)$ 所取之值的关系, 典型情况是与定

① 这里要除去在 $s=-2$, -4, $\cdots$ 处 $\varsigma(s)$ 的 "不足道" 的零点. —— 中译本注

义 $L(s)$ 的狄利克雷级数不收敛的点的关系上, 有很深刻的猜测! 这个现象的基本结果是 Birch-Swinnerton-Dyer 猜想[V.4], 它的弱的版本是: 与方程 (1) 相关的 L 函数在 $s=1$ 处为零, 当且仅当 (1) 有无穷多个解的 x 与 y 坐标都是有理数. 关于这个猜想已经知道了很多, 而且在 Deligne, Belinson, Bloch 和 Kato 的工作中已经大大推广, 然而在本文写作之时仍未解决.

III.48 李的理论 (Lie Theory)

Mark Ronan

1. 李群

为什么群在数学中如此重要? 一个主要的理由是: 可以通过了解一个数学结构的对称性来了解这个结构, 而一个已给的数学结构的对称性构成一个群. 有些数学结构是如此对称, 它不只有有限多个对称性, 而是其对称性形成了一个连续的族. 如果出现了这样的情况, 我们就进入了李群和李的理论的领域.

最简单的 "连续群" 的一个例子就是群 SO(2), 它是由 $\mathbf{R}^2$ 上所有绕原点的旋转构成的. 与 SO(2) 的每一个元素相连接的有一个角度 θ, 即所说的旋转的转角. 如果用 R_θ 表示逆时针方向旋转一个角 θ, 则这个群的群运算是由 $R_\theta R_\varphi = R_{\theta+\varphi}$ 给出的, 这里 $R_{2\pi}$ 理解为等于 R_0, 即群的恒等元.

群 SO(2) 不只是一个连续群, 还是一个李群. 粗略地说, 就是在此群中可以有意义地定义一条光滑曲线 (即一条不仅连续而且可微的曲线). 在 SO(2) 中任意给出两个元: R_θ 和 R_φ, 只要光滑地变动 θ 一直到变成 ϕ, 就定义了 SO(2) 中的一条光滑路径 (这种路径最显然的表示方法是用参数形式表示为 $R_{(1-t)\theta+t\varphi}$, 其中的 t 由 0 变到 1). 一个李群中的两个点并不一定都能用一条路径连接起来, 如果能够, 就说这个李群是**连通的**. 不连通李群的例子是 $O(2)$, 它是由 SO(2) 和它的反射构成的, 这里的反射是指的对于一条过原点的直线的反射. 任意两个旋转都可以用一条路径连接起来, 两个反射也是一样, 但是没有办法把一个旋转连续地变为一个反射.

李群是由李 (Sophus Lie, 1842—1899, 挪威数学家) 引入的, 原来的目的是为了对于微分方程建立伽罗瓦理论 [V.21] 的类似物. 由 $\mathbf{R}^n$ 或 $\mathbf{C}^n$ 上的可逆线性变换所成的李群, 例如上面的例子中的那一个, 称为**线性李群**, 而成为李群的一个重要的子类. 对于线性李群, 弄明白诸如 "连续" "可微" 或 "光滑" 这些词的含义是很容易的. 然而, 也可以考虑更抽象的李群 (实的或复的), 其元素不是用线性变换给出

的. 为了给出李群的完全一般的定义, 就需要*光滑流形*[I.3 §6.9] 的概念. 然而为简单起见, 我们主要限制于线性李群.

造出一个李群的一个很常用的方法是把一个空间中所有的保持某个或多个特定的几何结构的变换都收集来. 例如, **一般线性群** $\mathrm{GL}_n(\mathbf{R})$ 就定义为所有从 $\mathbf{R}^n$ 到 $\mathbf{R}^n$ 的可逆线性变换的群. **特殊线性群** $\mathrm{SL}_n(\mathbf{R})$ 则包含在其内, 即只留下其中保持体积和定向的可逆线性变换 (也就是*行列式*[III.15] 为 1 的线性变换) 所成的群. 如果只留下保持距离的线性变换, 就得到**正交群** $O(n)$. 如果既保持距离, 又保持定向, 就会得到**特殊正交群** $\mathrm{SO}(n)$, 很明显, 它就是 $\mathrm{SL}_n(\mathbf{R})\cap O(n)$. $\mathbf{R}^n$ 中的刚体运动 (就是保持距离和角的变换, 如旋转、反射和平移) 构成的**欧几里得群** $E(n)$ 是由正交群和平移群 (同构于 $\mathbf{R}^n$) 生成的. 如果把实数域 $\mathbf{R}$ 换成复数域 $\mathbf{C}$, 就有以上各个群在复域中的类比. 例如, $\mathrm{GL}_n(\mathbf{C})$ 就是空间 $\mathbf{C}^n$ 中所有可逆复线性变换的群, 而正交群 $O(n)$ 的复类比就是**酉群** $U(n)$. 还有**辛群** $\mathrm{Sp}(2n)$ 则是 $O(n)$ 和 $U(n)$ 在*四元数*[III.76] 上面的类比. 以上各个群, 除了 $E(n)$ 以外都是线性李群, 而要描述一个同构于 $E(n)$ 的线性李群也相当容易.

李群的许多重要的例子都是有限维的. 这句话粗略的意思就是, 它们可以用有限多个连续变化的参数来表示 (无限维李群虽然重要, 却较难掌握, 所以这里不来细说). 例如, $\mathrm{SO}(3)$, 即 $\mathbf{R}^3$ 中绕原点的旋转的群, 就是 3 维的. 每一个这种旋转都可以用 3 个参数① 来表示. 例如, 可以把这个旋转分解为绕 x 轴、y 轴和 z 轴的旋转. 飞机驾驶员都知道这三种旋转, 如果令飞机机身的轴为 x 轴, 这三种旋转分别称为 “滚翻”(roll)、“俯仰”(pitch) 和 “偏航”(yaw). 确定每一种旋转只需要一个参数, 即旋转角. 但是确定飞机的旋转不能用这三个角为参数, 因为它们不是独立的. 找出独立参数的方法之一是用两个参数 (例如用球坐标中的两个角) 来确定轴的方向, 再有第三个参数, 即旋转角. 可以取旋转角 θ 总是非负的, 即适合不等式 $0\leqslant\theta<\pi$(旋转一个大于 π 的角度和向反方向旋转一个小于 π 的角度的效果是一样的).

我们可以用几何方法来描述 $\mathrm{SO}(3)$ 如下: 令 B 为 $\mathbf{R}^3$ 中以原点为中心、π 为半径的球体. 给定 B 中非球心的点 P, 则此点可以表示 $\mathbf{R}^3$ 中的绕原点的以 OP 为轴旋转角即 OP 之长的旋转. O 本身表示恒等映射, 而球面上的两个对径点 P 和 P' 之间相差一个旋转角为 π 的旋转, [所以从效果来看, 对于球面上的这两点, OP 和 OP' 的效果是一样的. 这样, 我们应该把这两点粘在一起. 这样就看到了 $\mathrm{SO}(3)$ 作为一个*拓扑空间*[III.90] 和*射影空间*[I.3 §6.7] $\mathbf{RP}^3$ 是一样的. 与它比较起来, $\mathrm{SO}(2)$ 就简单多了, 它在拓扑上等价于一个圆周.

---

① 这里要注意, 原书并没有说这 3 个旋转角 (θ_x, θ_y, θ_z) 是参数. 因为说一个李群是 3 维的, 就要求这 3 个参数是独立的. 但是在现在的情况, 有 $\cos^2\theta_x+\cos^2\theta_y+\cos^2\theta_z=1$. 所以下面又讲了如何确定 3 个独立参数的问题. —— 中译本注

李群出现在许多涉及连续运动的学科中. 例如, 它出现在一些应用主题如导航系统的设计中, 也出现在一些非常 "纯粹" 的主题, 例如几何或微分方程中. 李群以及与之密切相关的下面就要讲到的李代数, 也时常出现在量子力学和其他物理分支的一些类型的代数结构里.

2. 李代数

正如上面的例子表明的那样, 李群时常是 "弯曲" 的, 而且具有非平凡的拓扑结构. 然而, 把李群与一个平坦的空间联系起来分析时常是有意义的, 这个平坦的空间就是李代数, 这里的想法和以下的想法有点类似: 在研究一个对称的结构例如球面时, 先去研究球面和它的一个切空间的关系. 对于李群, 我们要用的李代数就是李群在恒等元处的切空间, 可以把这个切空间看成李群的 "对数".

为了看清李代数是怎样出现的, 不妨考虑一个线性李群. 这个群的元素可以看作是某个向量空间上的线性变换, 或者等价地, (当选定了一个坐标系以后) 看成是一个方形的矩阵. 一般说来, 两个矩阵 A 和 B 的乘法是不可交换的 (就是说, 一般说来 AB 不一定会等于 BA). 但是, 如果考虑与恒等矩阵很接近的矩阵, 情况就会简单得多. 如果 $A=I+\varepsilon X$, 而 $B=I+\varepsilon Y$, 这里 ε 是很小的正数, 而 X, Y 是固定的矩阵, 则

$$AB=I+\varepsilon(X+Y)+\varepsilon^2XY,$$

而

$$BA=I+\varepsilon(X+Y)+\varepsilon^2YX\ .$$

如果略去含 ε^2 的项, 就会发现 A 和 B"几乎可换", A 和 B 的乘法 "几乎相当于"X, Y 的加法, 这非常类似于 A 和 B 的对数.

现在非正式地定义一个线性李群 G 的李代数就是所有矩阵 X 的集合, 使得对于充分小的 ε, 矩阵 $I+\varepsilon X$ 除有 ε^2 阶的误差以外, 位于 G 中, 例如, 一般线性群 $\mathrm{GL}_n(\mathbf{C})$ 的李代数 $\mathrm{gl}_n(\mathbf{C})$ 就是 $n\times n$ 复矩阵的集合. 可以把李代数看成是群 G 中的运动的一切可能的瞬时方向与速率的集合, 更精确的定义则是 G 中所有经过恒等元素 $R_0\in G$ 的光滑曲线 $\varepsilon\mapsto R_\varepsilon\in G$ 在 R_0 处的导映射 R_0' 的集合. 这个定义可以推广到更一般的抽象李群而没有太大的困难 (回到飞机驾驶员的例子, 李群 SO(3) 的元素可以用来描述飞机相对于固定坐标系的现时的定向, 而李代数 so (3) 的元素, 则可以用来描述驾驶员为了光滑地改变飞机的定向, 而施加于飞机的现时的翻滚、俯仰和偏航的速率).

正如我们看见的, 一般线性群 $\mathrm{GL}_n(\mathbf{C})$ 的李代数 $\mathrm{gl}_n(\mathbf{C})$ 就是所有 $n\times n$ 复矩阵的集合. 特殊线性群 $\mathrm{SL}_n(\mathbf{C})$ 的李代数 $\mathrm{sl}_n(\mathbf{C})$ 则是迹为 0 的复矩阵所成的子集合. 这是因为除了一个 ε^2 阶的误差以外, $\det(I+\varepsilon X)=1+\varepsilon\mathrm{tr}X$, 所以如果

$\varepsilon \mapsto I+\varepsilon X$ 是群中的一条路径, 则 $\mathrm{tr}X=0$. SO(n) 的李代数 so(n) 等于 $O(n)$ 的李代数 $o(n)$, 二者都是所有斜对称矩阵的集合. 类似地, SU(n) 的李代数 su(n) 和 $U(n)$ 的李代数 $u(n)$ 一样, 都是斜厄尔米特矩阵的集合 (所谓斜厄尔米特矩阵 $A=(a_{ij})$, 就是等于其自身的复共轭转置矩阵 (conjugate transpose matrix) 的反号的矩阵, 即有 $A=-A^*, A^*=(\bar{a}_{ji})$).

李群在乘法运算下为封闭这件事实, 可以用来证明李代数在加法运算下也是封闭的. 所以, 一个李代数就是一个 (实) 向量空间. 但是, 它还有外加的结构, 使它**远不仅**是向量空间. 例如, 设 A 和 B 是李群 G 的两个元素, 而且都很接近于恒等元. 于是, 可以找到一个很小的 ε 和李代数 g 的两个元素 X 和 Y, 使得 $A\approx I+\varepsilon X, B\approx I+\varepsilon Y$. 稍用一点线性代数, 就知道 A 和 B 的**交换子**$ABA^{-1}B^{-1}$(交换子可以用来量度 A 和 B 不可交换的程度) 可以用 $I+\varepsilon^2[X, Y]$ 来逼近, 这里 $[X, Y]=XY-YX$. $[X, Y]$ 这个量称为 X 和 Y 的**李括号**. 不严格地说, [因为 X 和 Y 分别表示群元素相应的切向量, 可以认为它们表示这些方向上的无穷小运动, 所以 $[X, Y]$ 表示先沿 X 方向运动, 再沿 Y 方向运动的结果与反转其次序, 先沿 Y 方向运动, 再沿 X 方向运动的结果二者之差].

李括号满足好几个漂亮的恒等式, 如反对称恒等式 $[X, Y]=-[Y, X]$, 而特别重要的是**雅可比恒等式**:

$$[[X, Y], Z]+[[Y, Z], X]+[[Z, X], Y]=0.$$

事实上, 可以用这些恒等式以完全抽象的方式来定义李代数, 正如我们曾以一些恒等式作为公理来定义其他代数对象, 如群、环、域那样. 但是在此不打算集中注意于李代数的这种抽象处理. [我们只提一提这种抽象处理的一个例子]: 有一个我们熟悉的李代数, 就是 $\mathbf{R}^3$, 其中定义李括号 $[x, y]$ 即为向量 x, y 的向量积: $x\times y$. 注意, 李括号一般不满足结合律 (除非是在平凡的情况).

我们已经看到, 线性李群 G 自然地在其李代数 g 上生成一个括号运算 $[\cdot, \cdot]$. 反过来, 一个李群如果是连通的, 则几乎可以从它的李代数来重构出这个李群, 其中已经有了加法、标量乘法和李括号运算. 更准确地说, 李群的任意元素 A 一定可以表示为其李代数的某个元 X 的指数[III.25] $\exp(X)$. 例如, 设这个李群是 SO(2), 可以把它与复平面 $\mathbf{C}$(就是前面提到过的 $\mathbf{R}^2$) 上的单位圆周等同起来. 这个圆周在 1 处的切线是铅直直线, 所以, 又可以把相应的李代数与纯虚数的集合 i$\mathbf{R}$ 等同起来 (但是, 通常的说法是: 其李代数就是 $\mathbf{R}$). 旋转一个角度 θ, 于是就可以写成 $\exp(\mathrm{i}\theta)$. 注意, 这种表示并非唯一的, 因为 $\exp(\mathrm{i}\theta)=\exp(\mathrm{i}(\theta+2\pi))$. 不难看到, 李群 $\mathbf{R}$ 的李代数也是 $\mathbf{R}$(为了使得这一点看起来有意义, 最好把李群 $\mathbf{R}$ 换成正实数的乘法群, 这个乘法群是同构于 $\mathbf{R}$ 的), 对于这个李群, 指数表达式却是唯一的. 一般说来, 如果两个连通的李群具有相同的李代数, 这些李群有共同的万有覆叠 (universal

covering), 因此彼此有密切的关联.

在线性李群情况下, 指数可以用我们熟悉的公式写为

$$\exp(X) = \lim_{n \to \infty}\left(1 + \frac{X}{n}\right)^n .$$

对于更抽象的李群, 指数最好是用常微分方程的语言来表述[①], 就是利用来自一元微积分学的恒等式

$$\frac{\mathrm{d}}{\mathrm{d}t}\mathrm{e}^{tX} = X\mathrm{e}^{tX}$$

的适当推广. 然而, 由于李群中的群运算的不可交换性, 关系式 $\exp(X+Y) = \exp(X)\exp(Y)$ 一般不成立, 这里正确的恒等式是 Baker-Cambell-Hausdorff **公式**:

$$\exp(X)\exp(Y) = \exp(X+Y) + \frac{1}{2}[X\ ,\ Y] + \cdots ,$$

省略号里面是含有李括号的相当复杂的无穷级数. 把李群和李代数联系起来的指数映射与李括号密切相关, 正因为如此, 想要对李群进行研究和分类, 可以先对李代数及其括号运算进行研究和分类.

3. 分类

对一个数学结构进行分类总是有意义的, 特别当这个结构很重要, 而分类又不是一望即知的, 就更加如此了. 按照这个判据, 关于李代数的分类的已经得到的结果, 无可否认是有趣的, 而且自 20 世纪初以来, 一直被认为是一项重大的数学成就.

因此, 对复的李代数, 即如 $\mathrm{sl}_n(\mathbf{C})$ 这样具有复向量空间结构的李代数, 进行分类比较容易. 每一个实的 n 维李代数都可以嵌入到一个复李代数中, 其复维为 n, 所以其实维要加一倍, 而为 $2n$. 这个嵌入称为原来的实李代数的**复化**(complexification). 然而, 同一个复李代数可以是多个实李代数 (称为这个复李代数的**实形式**) 的复化.

在对李群和李代数进行分类时, 第一步是限制在**单**(simple) **李群**和**单李代数**的情况. 所谓"单", 就是说它们不能再分解为更小的分支. 例如, 欧几里得群 $E(n)$ 包含了平移群 $\mathbf{R}^n$ 为其正规子群, 如果用它做商群而把它作为因子分出去, 就会得到正交群 $O(n)$, 所以 $E(n)$ 不是单李群. 形式地说, 一个李群为**单**, 如果它不包含真的连通正规子群, 一个李代数为**单**, 如果它不包含真*理想*[III.81 §2]. 在这个意义下, 李群 $\mathrm{SL}_n(\mathbf{C})$ 及其李代数 $\mathrm{sl}_n(\mathbf{C})$ 对任意的 n 均为单的. 有限维复单李代数是由基灵 (Wilhelm Karl Joseph Killing, 1847–1923, 德国数学家) 和*嘉当*(Élie Joseph Cartan, 1869–1951, 法国数学家)[VI.69] 在 1888–1894 年间作了分类的.

---

① 其实, 李群和李代数是描述常和偏微分方程的代数侧面的最好的工具, 这种方程在时间中的演化可以以一个李群为模型, 而用于表述这个方程的微分算子则可用相关的李代数为模型. 然而, 我们不打算在这里讨论李的理论和微分方程的重要联系.

这种分类时常是放置在所谓**半单**李代数的背景下进行的, 所谓半单李代数就是可以用唯一的方式 (次序不计) 来分解为单李代数的直和的李代数, 如同自然数可以唯一分解为素数的乘积那样. 此外, 莱维 (Levi) 定理指出, 一个一般的有限维李代数 g 都可以表示为一个半单代数 (称为 g 的**莱维子代数**) 和一个可解子代数 (称为 g 的**根**(radical)) 的组合 (更准确的称呼是"半直积"). 可解李代数和群论中的可*解群*[V.21] 相关, 是很难分类的, 但是在许多应用中, 可以限于只关注半单李代数, 从而也只关注单李代数.

一个单李代数 g 可以分裂为较小的子代数, 它们不是理想, 但是以一种特别漂亮的方式互相有关. sl_{n+1} 的情况是典型的, 我们就用它来解释一般的理论. sl_{n+1} 是由迹为 0 的 $(n+1)\times(n+1)$ 矩阵构成的, 它可以用以下的方式分解为直和

$$\mathrm{sl}_{n+1} = n_+ \oplus h \oplus n_-,$$

其中 h 是迹为 0 的对角矩阵的集合, n_+ 和 n_- 分别是上三角矩阵和下三角矩阵而且对角线上的元素全为 0 的矩阵的集合. 两个对角矩阵 X 和 Y 是可交换的, 所以它们的李括号 $[X\,,\,Y] = XY - YX$ 为 0. 换言之, 如果 X 和 Y 都属于 h, 则 $[X\,,\,Y] = 0$. 一个李代数, 如果对所有的元素 X 和 Y 都有 $[X\,,\,Y] = 0$, 就说它是**阿贝尔的**.

每一个单李代数 g 都有类似的分解, 而子空间 h 是一个极大阿贝尔子代数, 称为**嘉当子代数**(对于非单李代数, 嘉当子代数的定义比较复杂). 嘉当子代数之所以重要, 是因为它们对其余的李代数上的作用可以同时对角化. 这句话的意思是: h 的一个余集合可以分裂为 1 维的成分 g_α, 称为**根空间**, 它们在 h 的作用下不变. 换一个方法来说, 就是如果 X 属于 h, 而 Y 属于某个根空间, 则 $[X\,,\,Y]$ 是 Y 的一个标量倍 (对角化要用到*代数的基本定理*[V.13], 这就是我们规定要处理复李代数的原因).

对于 sl_{n+1}, 这件事是这样做的. 每一个根空间 g_{ij} 就是这样的矩阵所成的 1 维空间: 这些矩阵除了第 i 行、第 j 列的一个元以外全为 0. 如果 $X \in h$(即以 0 为迹的对角矩阵), 而 $Y \in g_{ij}$, 这时不难验证 $[X\,,\,Y]$ 也在 g_{ij} 中. 事实上,

$$[X\,,\,Y] = (X_{ii} - X_{jj})Y\ .$$

如果把 X 顺着对角线往下读, 则可以把 X 和一个向量等同起来, 而 X 的对角线上的元素就依次是这个向量的各个坐标 X_{ii}, 而如果用 e_i 表示第 i 个坐标为 1 其余坐标为 0 的向量, 则 $X_{ii} - X_{jj}$ 可以写成 $(e_i - e_j\,,\,X)$. 把向量 $e_i - e_j$ 称为根向量.

一般的复半单李代数 g 都可以用它的根向量 α 和根空间 g_α 来描述. g 的**秩**等于嘉当子代数 h 的维数, 也等于由根向量所张的向量空间的维数. 例如 sl_{n+1} 的秩是 n, 而我们已经看到其根向量就是向量 $e_i - e_j$. 根向量的集合远非任意的: 它们

要服从一些简单的然而很有限制性的几何性质. 特别是如果把根向量 α 对垂直于另一根向量 β 的超平面作反射, 其结果 $s_\beta(\alpha)$ 将是第三个根向量, 这里的 s_β 就表示上面说的反射 (要想把上面说的“垂直”说清楚, 就需要在嘉当子代数上定义一个特殊的内积, 称为**基灵形式**, 但是我们不在这里讨论这个问题). 这些反射构成一个群, 称为外尔群. 根向量构成所谓**根系**, 上面所说的几何性质就使得我们能够对根系进行分类, 从而也就能够对所有的复半单李代数进行分类. 这个分类可以用一个很简单的图式来表示, 这个图式称为邓肯 (Dynkin, 即 Eugene Borisovich Dynkin, 1924–, 前苏联数学家) 图. 见图 1.

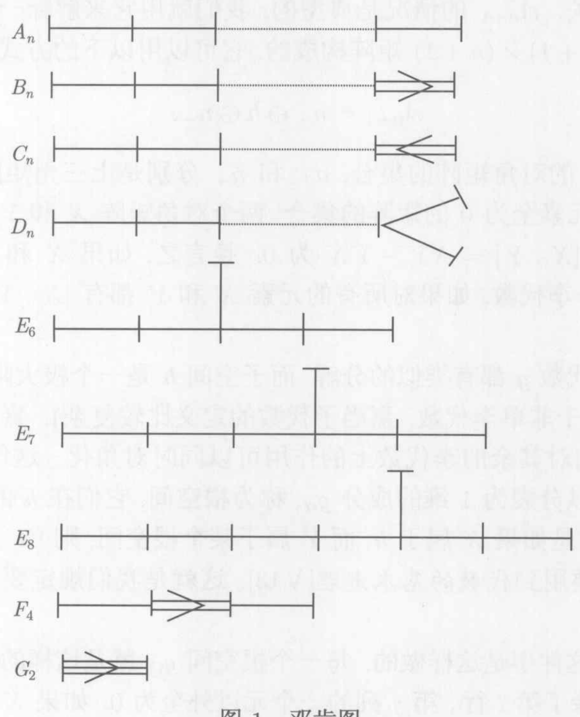


图 1 邓肯图

图上的结点相应于所谓**单根**. 每一个根都是单根的线性组合, 其系数或者全为非负, 或者全为非正. 两个结点之间的键 (或者没有键) 决定了相应单根的内积. 如果没有键, 就是指相应内积为 0, 如果有单键, 就是指这两个根向量长度相同, 而其夹角为 120°. 一个图式上如果只有单键, 指根向量在 $\mathbf{R}^n$ 中张了一族直线, 而任意两条直线的夹角或为 90° 或为 60°. 在 B_n , C_n , F_4 和 G_2 的图式中, 有几对结点之间画了箭头, 这时, 箭头表示从长的向量指向短向量; 在 B_n , C_n , F_4 的情况, 长度之比是 $\sqrt{2}$, 而在 G_2 的情况, 则是 $\sqrt{3}$. 在这 4 个情况下, 根向量的长度均有两个情况, 而在仅有单键的情况, 所有根向量的长度都是相同的.

A_n 的图式画的是 sl_{n+1}, 它的单根是 $e_i - e_{i+1}$, $1 \leqslant i \leqslant n$, 在图上就是由左到右的各个结点. 注意, 如果两个单根在图上是不互相邻接的, 其内积必为 0, 而当它们相邻接时, 则为 -1. 每一个根 $e_i - e_j$ 均为图上的一个连通的线段上的单根之和, 而系数或全为 1, 或全为 -1.

4 个无穷族 A_n , B_n, C_n 和 D_n 相应于**经典的李代数**, 它们的实形式分别是 $\mathrm{sl}_{n+1}(\mathbf{R})$, $\mathrm{so}(2n+1)$, $\mathrm{sp}(2n)$ 和 $\mathrm{so}(2n)$, 即**经典李群** $\mathrm{SL}_{n+1}(\mathbf{R})$, $\mathrm{SO}(2n+1)$, $\mathrm{Sp}(2n)$ 和 $\mathrm{SO}(2n)$ 的李代数.

前面已经提到, 秩为 n 的单李代数 g 可以分解为一个 n 维的嘉当子代数和一组 1 维根空间的直和, 而每一个根空间又相应于一个根. 由此可得

$$\dim g = g \text{ 的秩} + \text{根的个数}.$$

下面就是单李代数的维数:

$$\begin{aligned}
&\dim A_n = n + n(n+1) = n(n+2), \\
&\dim B_n = n + 2n^2 = n(2n+1), \\
&\dim C_n = n + 2n^2 = n(2n+1), \\
&\dim D_n = n + 2n(n-1) = n(2n-1), \\
&\dim G_2 = 2 + 12 = 14, \\
&\dim F_4 = 4 + 48 = 52, \\
&\dim E_6 = 6 + 72 = 78, \\
&\dim E_7 = 7 + 126 = 133, \\
&\dim E_8 = 8 + 240 = 248.
\end{aligned}$$

图式的每一个结点都相应于一个单根, 因此也就相应于越过一个超平面的反射, 这个超平面垂直于那个根, 这些反射就以特别漂亮的方式构成外尔群 W. 若以 s_i 表示结点 i 的反射, 则 W 就由这些阶为 2 的元素 s_i 生成, 它们只服从下面的关系:

$$(s_i s_j)^{m_{ij}} = 1 ,$$

m_{ij} 就是 $s_i s_j$ 的阶 (关于生成元和关系的讨论可见 [IV.10§2]). 这些阶可以从图式中按以下的规则来决定:

(i) 如果没有键, 则 $s_i s_j$ 的阶为 2;

(ii) 如果有单键, 则 $s_i s_j$ 的阶为 3;

(iii) 如果有双键, 则 $s_i s_j$ 为 4;

(iv) 如果有 3 重键, 则 $s_i s_j$ 的阶为 6.

例如, A_n 型的外尔群同构于对称群[III.68]S_{n+1}, 而可以取 s_1 , $\cdots$, s_n 为对换 (transposition)(1 , 2) , (2 , 3) , $\cdots$, $(n, n+1)$. 注意 B_n 和 C_n 根系的邓肯图示给出同样的外尔群.

从这种根系的分类, 原则上可以得到对所有的有限维半单李代数和李群的分类. 然而, 关于半单李代数和李群仍有一些基本问题只是部分地得到了理解. 例如, 李的理论的一个特别重要的目的是了解一个给定的李代数或李群的线性表示. 所谓线性表示, 粗略地说就是通过对抽象李群或李代数的元指定一个矩阵, 这样来解释这个抽象李群或李代数. 虽然所有的单李群或单李代数的表示都已经分类了, 并得到了显式的描述, 这些描述用起来却并非易事, 而基本问题 (例如, 怎样把一个给定的表示分解为较简单的表示) 的回答需要代数组合学的一些精巧的工具.

上述的根系理论, 可以推广到无限维李代数的一个很重要的类, 即卡茨–穆迪 (Kac-Moody) 代数, 这种代数出现在好些物理领域 (如条目顶点算子代数[IV.17] 所描述的) 和代数组合学里.

III.49　线性与非线性波以及孤子 (Linear and Nonlinear Waves and Solitons)

Richard S. Palais

1. 罗素和巨大的平移波

对于广大世人来说, 罗素 (John Scott Russell, 1808–1882) 也就是一位苏格兰造船工程师, 他在 1865 年建造了当时最大的轮船 "**大东号**"(The Great Eastern). 但是当这件事慢慢地淡出人们的记忆以后, 罗素却被人们作为一位数学家记在心里. 他虽然只受到过有限的数学训练, 却是第一个认识到高度重要的数学概念即现在所说的**孤子**的人, 而他当时称之为 "巨大的平移波". 下面就是一段常为人们引用的话, 他在其中讲述了自己是怎样认识了它的. [这段话出自本文后的文献 (Russell, 1844)].

> 我正在观察船的运动, 两匹马拉着它在狭窄的运河里快速地前进, 那时, 船突然停下来了 —— 但是船所激起的运河里的水体并没有停下来, 它聚集在船头边上, 剧烈地湍动着, 突然把船抛在后面, 以巨大的速度滚动向前, 形状是一个孤独的隆起, 如同一堆圆圆的光滑的界限分明的水堆, 沿着运河继续它的航程, 既不改变形状, 也不减少速度. 我骑着马跟了上去, 它仍然以大约每小时八至九英里的速度滚动向前, 保持着原来的长度大约三十英尺、高度一英尺到一英尺半的形状. 它的高度逐渐地减小, 我追了它一到两英里, 它才在运河弯曲处消失了. 这样, 在 1834 年 8 月, 我第一次有幸拜会了这个奇异而美丽的现象, 我把它叫做平移波.

您可能觉得罗素在这里描写的现象没有什么不平常, 而事实上, 在那以前或以后, 有许多人都看见过这个景象的演示, 而没有注意到什么不平常的事情. 但是, 罗素对

于水波非常熟悉, 而且具有科学家的敏锐的观察眼光. 触动他的是: 在运行很长的距离以后, 这个头波仍然具有引人注意的**稳定性**. 他知道, 如果在例如一个平静的湖面上激起了一个行波, 它就会很快地散开成为一串小小的涟漪, 而不会成为一个单独的 "水堆", 继续走很长的距离. 关于在狭窄的浅浅的渠道里行走的水波, 一定有什么很特别的地方.

罗素为自己的发现着迷了 —— 甚至是有点困惑. 他在自己家的后院里建造了一个水箱, 广泛地做起了实验, 并把结果的数据和草图记录在笔记本里. 例如, 他发现了孤子的速度依赖于其高度, 甚至发现了速度作为高度的函数的正确公式. 更加惊人的是, 在罗素的笔记本里, 可以找到两个孤子互相作用的惊人的草图. 这件事在一百多年后为人重新发现是 KdV 方程的严格解的时候, 引起了惊奇 (见下面第 3 节).

然而, 我们将会看到, 孤子是非常的非线性的现象, 而当罗素时代最好的数学家, 尤其值得提到的有斯托克斯和艾里 (Sir George Biddell Airy , 1801–1892, 英国数学家) 都试图用水波的线性理论来理解罗素的观察, 而在当时又只能得到这样的理论, 所以, 他们都没有发现任何像孤子这样的性态的踪迹, 甚至表示对于罗素之所见是否真实还有疑问.

直到罗素死后, 由于布西内斯克 (Joseph Valentin Boussinesq, 1842–1929, 法国数学家和力学家)1871 年的工作, 特别是 Korteweg (Diederick Johannes Korteweg, 1848–1941, 荷兰数学家) 和de Vries (Gustav de Vries, 1866–1934, 荷兰数学家) 在 1894 年合写的论文, 才终于发现罗素的细心的观察和实验与数学理论完全一致. 又过了七十多年, 这个巨大的平移波的全部重要性才为人们认识, 这以后, 它就成了 20 世纪余下的年代里密集研究的对象.

2. Korteweg-de Vries 方程

Korteweg 和 de Vries 是最先导出描述浅的渠道里水波的适当的微分方程的人, 我们可以把他们的方程 (通常称为 KdV 方程) 写成下面的简洁的形式:

$$u_t + uu_x + \delta^2 u_{xxx} = 0,$$

这里 u 是两个变量 x 和 t, 分别代表空间和时间的函数. "空间" 是 1 维的, 所以 x 是一个实数, 而 $u(x, t)$ 表示波在 x 处和时刻 t 的高度. 记号 u_t 是 $\partial u/\partial t$ 的简写, u_x 代表 $\partial u/\partial x$, 而 u_{xxx} 则代表 $\partial^3 u/\partial x^3$.

这是演化方程的一个例子, 如果对每一个 t, 用 $u(t)$ 表示一个由 $\mathbf{R}$ 到 $\mathbf{R}$ 映 x 为 $u(x, t)$ 的函数, 则这个方程表示 $u(t)$ 怎样随时间 "演化". 一个演化方程的柯西问题, 就是用关于初值 $u(0)$ 的知识来决定这个演化的问题.

2.1 一些模型方程

为了对 KdV 方程有一个通观, 简略地看另外三个演化方程是有好处的. 第一

个是经典的*波方程*[I.3 §5.4]

$$u_{tt}-c^2u_{xx}=0\,.$$

要解这个方程的柯西问题, 首先对波算子 $(\partial^2/\partial t^2)-c^2(\partial^2/\partial x^2)$ 作 "因子" 分解, 把它写成一个乘积 $((\partial/\partial t)-c(\partial/\partial x))((\partial/\partial t)+c(\partial/\partial x))$. 然后转换到所谓特征坐标 $\xi=x-ct$ 和 $\eta=x+ct$. 这样, 原来的方程就变成了 $\partial^2u/\partial\xi\partial\eta=0$, 很明显, 它有通解 $u(\xi,\eta)=F(\xi)+G(\eta)$. 回到 "实验室坐标" x, t, 通解就成了 $u(x,t)=F(x-ct)+G(x+ct)$. 如果波的初始波形是 $u(x,0)=u_0(x)$, 而初速是 $u_t(x,0)=v_0(x)$, 作一些简单的计算就可以得出

$$u(x,t)=\frac{1}{2}\left[u_0(x-ct)+u_0(x+ct)\right]+\frac{1}{2}\int_{x-ct}^{x+ct}v_0(\xi)\,\mathrm{d}\xi\,,$$

此式称为波方程的 "达朗贝尔解".

请注意重要的 "拨弦" 情况, 即 $v_0=0$ 的情况. 这时, 波的初始的剖面分裂成两个 "行波" 之和, 而每一个行波的剖面都同为 $\frac{1}{2}u_0$, 一个向左传播, 一个向右传播, 而速率同为 c. 按照以下的提示来计算一下达朗贝尔解是一个简单的练习: 因为 $u_0(x)=F(x)+G(x)$, 所以 $u_0'(x)=F'(x)+G'(x)$, 而 $v_0(x)=u_t(x,0)=-cF'(x)+cG'(x)$.

第二个要考虑的方程是

$$u_t=-u_{xxx}\,, \tag{1}$$

它是从 KdV 方程中略去非线性项 uu_x 得到的. 这个方程不仅是线性的, 而且是对平移不变的 (意思是, 如果 $u(x,t)$ 是一个解, 则对任意常数 x_0 和 t_0, $u(x-x_0,t-t_0)$ 也是解). 这种方程可以用*傅里叶变换*[III.27] 来求解, 我们试着来求它的形如 $u(x,t)=\mathrm{e}^{\mathrm{i}(kx-\omega t)}$ 的 "平面波" 解. 把这个式子代入 (1), 就会得到等式

$$-\mathrm{i}\omega\mathrm{e}^{\mathrm{i}(kx-\omega t)}=\mathrm{i}k^3\mathrm{e}^{\mathrm{i}(kx-\omega t)}$$

并由此得到一个简单的代数方程 $\omega+k^3=0$. 这个式子称为 (1) 的 "**色散关系**" (dispersion relation), 借助于傅里叶变换, 不难证明每一个解都是形如 $\mathrm{e}^{\mathrm{i}(kx-\omega t)}$ 的解的叠加, 而色散关系告诉我们, 在每一个这种基本的解中 "波数" k 与 "角频率" ω 的关系.

函数 $\mathrm{e}^{\mathrm{i}(kx-\omega t)}$ 表示一个行进速度为 ω/k 的波, 而我们所已经证明的就是这个速度即 $-k^2$. 所以这个解的不同的平面波成分以不同速度前进, 角频率越高, 速度也就越大. 由于这个原因, 方程 (1) 被称为是**色散的**.

如果在 KdV 方程中略去 u_{xxx} 又会发生什么情况? 这时, 得到的是所谓**无粘性的伯格**(Burger)**方程**:

$$u_t+uu_x=0\,. \tag{2}$$

uu_x 这一项可以重写为 $\frac{1}{2}\left(u^2\right)_x$. 现在考虑作为 t 的函数的积分 $\int_{-\infty}^{\infty} u(x, t)\,\mathrm{d}x$. 它的导数是 $\int_{-\infty}^{\infty} u_t\mathrm{d}x$, 而由 (2) 式, 应该等于

$$-\int_{-\infty}^{\infty}\frac{\partial}{\partial x}\left(\frac{1}{2}u^2\right)\mathrm{d}x=\left[-\frac{1}{2}u(x, t)^2\right]_{-\infty}^{\infty}.$$

所以, 如果 $\frac{1}{2}u(x, t)^2$ 在无穷远处为 0, 则 $\int_{-\infty}^{\infty} u(x, t)\,\mathrm{d}x$ 是一个"运动常量", 而我们就说, 无粘性的伯格方程是一个**守恒律** (在这里使用的论据可以用于任意的形如 $u_t=(F(u))_x$ 的方程, 这里 F 是 u 和 u_x 的光滑函数. 这种方程称为广义守恒律. 例如取 $F(u)=-\left(\frac{1}{2}u^2+u_{xx}\right)$ 就会得到 KdV 方程).

无粘性的伯格方程 (和其他的 F 仅含 u 的守恒律) 可以用特征线方法求解. 这个方法的思想是: 在 xt 平面上找一条光滑曲线 $(x(s), t(s))$, 使得柯西问题的解沿这条曲线取常值. 设有 s 之值 s_0, 使 $t(s_0)=0$, 又记 $x_0=x(s_0)$, 于是, 解 $u(x, t)$ 在这条曲线上的值应该是 $u(x_0, 0)$, 而我们用 $u_0(x_0)$ 去记它. 这种曲线称为**特征曲线**, 而 $u(x, t)$ 沿着它的导数是 $(\mathrm{d}/\mathrm{d}s)\,u(x(s), t(s))=u_xx'+u_tt'$, 所以, 如果要求解沿这条曲线取常值, 就应该取这个导数为 0. 利用 $u_t=-uu_x$, 就会得到

$$\frac{\mathrm{d}x}{\mathrm{d}t}=\frac{x'(s)}{t'(s)}=-\frac{u_t}{u_x}=u(x(s), t(s))=u_0(x_0),$$

所以特征曲线是斜率为 $u_0(x_0)$ 的直线. 换句话说, u 沿着直线 $x=x_0+u_0(x_0)\,t$ 取常值 $u_0(x_0)$.

注意, 最后这个事实有下面的几何解释: 要找时刻 t 的波的剖面 (即映射 $x\mapsto u(x, t)$ 的图像), 只需把波在初始时刻的剖面上的点 $(x, u_0(x))$ 向右平移一个量 $u_0(x)t$ 即可. 现在来考虑初始剖面上 $u_0(x)$ 下降的部分, 于是初始剖面上更高的部分将以更大的速度平移 (因为 $u_0(x)$ 更大), [而且随着时间向前推移, 因为 t 也在变大, 所以平移的速度也更大], 所以初始剖面的负斜率变得"更负". 事实上, 在一段有限的时间以后, 波的早前的部分将会"追上"后来的部分, 这意味着我们将不再有一个函数的图像. 这个现象第一次出现的时间称为波的"破裂时间", 这时会看见波破裂开来. 这个过程通常称为**激波的形成**, 也就是**波的剖面从变陡到破裂**的过程.

2.2 步长的分裂

现在回到 KdV 方程本身: $u_t=-uu_x-u_{xxx}$(其中暂时设 $\delta^2=1$). 为什么会出现罗素首先在实验中观察到的引人注目的解的稳定性呢? 其原因在于在 u_{xxx} 的色散效应和 uu_x 的激波形成效应之间的平衡.

现在有一种处理这一类平衡的一般的技巧. 在纯粹数学圈子里, 它通常称为 Trotter **乘积公式**[①] 而在应用数学和计算数学圈子里, 则称为**步长分裂方法**. 它的初步的思想很简单：当 t 增加为 $t+\Delta t$ 时, 先把 u 变为 $u-u_{xxx}\Delta t$, 因为方程 $u_t=-u_{xxx}$ 要求这样做. 第二步再把它变为 $u-u_{xxx}\Delta t-uu_x\Delta t$, 这是由方程 $u_t=-uu_x$ 所要求的. 要想得到 $u(x,t)$, 就可从初始剖面开始, [把每一个步子都这样分裂为这两类步子, 并且交错地进行下去, 所以这个方法称为步长分裂法]. 最后再令步长趋于零而求极限.

步长的分类暗示了 KdV 方程里有一种 u_{xxx} 的色散效应和 uu_x 的激波形成效益得到平衡的机制. 可以设想波的剖面的演化是由一对一对如此的小步骤相继造成的：当 u , u_x 和 u_{xxx} 都不太大时, 变陡的机制起统治作用. 但是当时间进到破裂时间 T_B 附近时, u 仍然保持有界 (因为它是由 u_0 的各个部分水平地平移而成的). 不难证明最大斜率 (即 u_x 的最大值) 与 $(T_B-t)^{-1}$ 同阶, 而在这一点, u_{xxx} 则与 $(T_B-t)^{-5}$ 同阶. 这样在破裂时刻和破裂点附近, u_{xxx} 这一项把非线性和开始出现的激波都比下去了. 这样, 稳定性是由某种负反馈造成的. 计算机仿真表明, 演出的正是这么一个情节.

3. 孤子及其相互作用

我们刚才看见了 KdV 方程表示了一种来自三阶导数项的色散和来自非线性项的出现激波的倾向之间的平衡, 而事实上, 许多 1 维的物理系统, 如果其中同时出现了温和的色散和弱的非线性, 则它们时常在一定程度的近似之下可以用 KdV 方程为其模型.

Korteweg 和 de Vries 在 1894 年合写的文章里引入了 KdV 方程, 并且以使人信服的数学论据说明了它就是控制着浅渠道里的水波的方程. 他们也用显式的计算证明了这个方程允许有行波, 而且恰好具有罗素所描述的性质, 包括他在自己的水箱实验里决定出来的波的高度与速度的关系.

但是 KdV 方程的其他值得注意的性质之变得很明显却要晚得多. 1954 年, Fermi, Pasta 和 Ulam(以下简记为 FPU) 用一个非常初级的计算机, 就弦上的非线性恢复力作了数值试验, 而且在能量如何分布在这个系统的简正模式 (normal mode) 上, 他们得到的结果与当时流行的期望发生了矛盾. 十年后, Zabusky 和 Kruskal 在一篇著名的论文 (即后面所附的参考文献 (Zabusky, Kruskal, 1965) 中, 重新检验了 FPU 的结果, 并且指出, FPU 的弦可以用 KdV 方程来很好地逼近. 然后, 他们作

① Trotter 公式就是对于任意的自伴算子 A 和 B,

$$\mathrm{e}^{t(A+B)}=\lim_{n\to\infty}\left(\mathrm{e}^{tA/n}\cdot\mathrm{e}^{tB/n}\right)^n=\lim_{n\to\infty}\left[\left(\mathrm{e}^{tA/n}\cdot\mathrm{e}^{tB/n}\right)\cdots\left(\mathrm{e}^{tA/n}\cdot\mathrm{e}^{tB/n}\right)\right]\quad(n\text{个因子}).$$

也就是说, 虽然 $\mathrm{e}^{t(A+B)}$ 不能分成 e^{tA} 和 e^{tB}, 但是, 把 “步长” 缩小到 $1/n$ 后, 却 “基本上” 可以. 这里的收敛的意义需要详细论证. 这个公式在量子物理、计算数学等方面都有应用. —— 中译本注

了自己的计算机实验, 用相应于 FPU 实验的数据作初始值解出了 KdV 方程的柯西问题. 他们在这些仿真里面观察到 "孤子" 的第一个例子, 这个词也是他们创用的, 用以描述 KdV 方程的某些解所展现的一种值得注意的粒子似的性态 (弹性散射). Zabusky 和 Kruskal 说明了怎样用孤子的相干 (coherence) 来说明 Fermi, Pasta 和 Ulam 所观察到的一些非正常的结果. 但是, 他们在解决了那个神秘 [即那些非正常的结果的同时], 又引起了更神秘的问题: 就是 KdV 孤子的行为不像在应用数学里发现过的任何东西, 而探求对这些值得注意的行为的解释时引导到许多发现, 改变了应用数学后三十年的进程. 我们现在要对上面的概述补上一些数学细节, 先从 KdV 方程的显式解开始.

求 KdV 方程的行波解是直截了当的事. 先把行波解 $u(x, t)=f(x-ct)$ 代入 KdV 方程, 于是得到一个常微分方程 $-cf'+6ff'+f'''=0$. 如果加上要求解在无穷远处为零的边值条件, 经过常规的计算就可以得到以下的两参数行波解族:

$$u(x, t)=2a^2\operatorname{sech}^2\left(a\left(x-4a^2t+d\right)\right).$$

它们就是罗素所观察到的孤波, 而这些解通常称为 KdV 方程的 **1 孤子解**. 注意, 它们的振幅 $2a^2$ 正是速度 $4a^2$ 的一半, 而 "宽度" 与 a^{-1} 成正比. 所以更高的孤子一定更瘦, 移动也更快.

下一步, 可以按照 Toda 的办法 "导出"① KdV 方程的 **2 孤子解**. 先把 1 孤子解写为 $u(x, t)=2\left(\partial^2/\partial x^2\right)\log\cosh\left(a\left(x-4a^2t+\delta\right)\right)$, 或 $u(x, t)=2\left(\partial^2/\partial x^2\right)\times\log K(x, t)$, 其中 $K(x, t)=\left(1+\mathrm{e}^{2a\left(x-4a^2t+\delta\right)}\right)$. 现在要推广这一点来求方程以方程以下形式的解:

$$u(x, t)=2\left(\partial^2/\partial x^2\right)\log K(x, t),\quad K(x, t)=1+A_1\mathrm{e}^{2\eta_1}+A_2\mathrm{e}^{2\eta_2}+A_3\mathrm{e}^{2(\eta_1+\eta_2)},$$

而 $\eta_i=a_i\left(x-4a_i^2t+\delta_i\right)$, 把它代入 KdV 方程来看会得到什么. 可以验证, 对于任意的 A_1, A_2, a_1, a_2, δ_1, δ_2, 只要令 $A_3=\left(\dfrac{a_2-a_1}{a_1+a_2}\right)^2A_1A_2$, 这种形状的 $u(x, t)$ 就都能满足 KdV 方程. KdV 方程的这样得出的解, 就称为它的 2 孤子解.

现在可以证明对于这样选取的 a_1, a_2, 有

$$u(x, t)=12\frac{3+4\cosh(2x-8t)+\cosh(4x-64t)}{[\cosh(3x-36t)+3\cosh(x-28t)]^2}.$$

特别是, $u(x, 0)=6\operatorname{sech}^2(x)$. 当 t 是一个绝对值很大的负数时, $u(x, t)$ 渐近等于 $2\operatorname{sech}^2(x-4t-\phi)+8\operatorname{sech}^2(x-16t+\phi/2)$, 而当 t 是一个很大的正数时, $u(x, t)$ 渐近等于 $2\operatorname{sech}^2(x-4t+\phi)+8\operatorname{sech}^2(x-16t-\phi/2)$, 这里 $\phi=\log 3/3$.

① 这完全是一个骗局! 只有知道了解的形状, 才能聪明地选出 K 来.

请注意这里说的是什么. 如果追随着从 $-T$ 到 T 的演化 (这里 T 是一个很大的正数), 我们先看见的是两个 1 孤子: 左边的一个高些瘦些, [所以走得快些], 后来就追上了右边的一个矮些胖些 [但走得慢些] 的 1 孤子. 大约在 $t=0$ 时候, 两个孤子合成了一个驼峰 (形状是 $6\text{sech}^2(x)$). 后来, 它们又分开了, 恢复了原来的形状, 但是高瘦个儿到了右边, [矮胖子落后到左边去了], 好像是互相穿透了一样. 它们的相互作用的唯一后果是各发生了一个相变: 慢的一个比原来的位置稍微滞后了一点, 而快的一个要稍微超前一点. 这里的最终结果除了发生相变这一点以外, 仍然是我们从线性相互作用所能够期望的. 只有在仔细地观察这两个孤子相遇时的相互作用, 才能看到其高度非线性的本质 (例如, 在 $t=0$ 时, 合成的波的最大振幅 6 要比合成前高一点的波的最大振幅 8 小). 但是, 最惊人的当然是这两个个别的孤子的恢复能力: 它们在碰撞以后又会还原, 不但是能量没有发射出去, 甚至波形也保持下来了 (值得注意的是在 (Russell, 1844, 384) 中就画了一个他在自己家的后院的水箱里做的 2 孤子相互作用实验的草图).

现在回到 Zabusky 和 Kruskal 的计算机实验. 由于数值的原因他们选择处理周期边值条件的情况. 事实上, 他们研究的是圆周上的 KdV 方程 $u_t+uu_x+\delta^2u_{xxx}=0$(引文即 1965 年的报告中所说的方程 (1) 就是指的这个方程). 在他们所发表的报告里, 取 $\delta=0.022$, 并且使用了初值 $u(x,0)=\cos(\pi x)$. 有了上面讲的背景知识, 再来读一下他们 1965 年的报告里的一段话就很有趣了, 在这个报告里第一次使用了 “孤子” 这个词:

> (Ⅰ) 一开始, (1) 中的前两项起主要作用, 出现了经典的追赶现象, 即是说在有负斜率的区域里 u 变陡了. (Ⅱ) 其次, 当 u 变得充分陡以后, 第三项变得很重要了, 从而阻止了间断性的发生. 相反, 在波前的左方发展了小波长的震荡. 这些震荡的振幅都在增长, 最后**每一个**震荡的振幅都几乎达到恒定 (它们从左到右线性地增加), 而具有 (1) 的单个的孤立波的形状. (Ⅲ) 最后, 每一个 “孤立波脉冲” 或称**孤子**开始匀速运动, 其速率 (相对于产生脉冲的 u 的背景值) 正比于其振幅. 这样, 孤子分散开来. 由于周期性, 两个或多个孤子在空间上互相追上, 而且非线性地互相作用. 在相互作用以后, 它们马上又各自重新出现, 大小与形状都基本没有改变. 换句话说, 每一个孤子都好像穿越了对方, 而身份不变. 在这里, 我们有了一个非线性的物理过程, 在其中, 互相作用的局部化的脉冲并没有不可逆地散射开来.

进一步阅读的文献

Lax P D. 1996. *Outline of a Theory of the KdV Equation in Recent Mathematical Methods in Nonlinear Wave Propagation*. Lecture Notes in Mathematics New York: Springer,

1640:70-102.

Palais R S. 1997. The symmetries of solitons. *Bulletin of the American Mathematical Society*, 34: 339-403.

Russell J S. Report on waves. In *Report of the 14th Meeting of the British Association for the Advancement of Science*. London: John Murray, 311-390

Toda M. 1989. *Nonlinear Waves and Solitons*. Dordrecht: Kluwer.

Zabusky N J, and Kruskal M D. 1965. Interaction of solitons in a collisionless plasma and the recurrence of initial states. *Physic Review Letters*, 15: 240-243.

III.50 线性算子及其性质 (Linear Operators and Their Properties)

1. 线性算子的一些例子

两个向量空间[I.3 §2.3]V 和 W 之间的线性映射[I.3 §4.2] 就是一个满足下面条件的函数 $T: V\rightarrow W$:$T(\lambda_1v_1+\lambda_2v_2)=\lambda_1Tv_1+\lambda_2Tv_2$. 有两个短语几乎和“线性映射”可以完全互换地使用, 就是“线性变换”和“线性算子”. 当想要强调线性映射在某个其他对象上的作用效果时, 就常用线性变换. 例如, 时常用“变换”一词来讲诸如旋转或反射这些几何运算. 而当讲到无限维空间之间的线性映射时, 特别是当这个映射是构成一个代数的一元时,“算子”一词则是首选. 下面讨论的就是这一类线性映射.

从线性算子的一些例子开始.

(i) 若 X 是一个巴拿赫空间[III.62], 其元素是一些无穷序列, 则可以定义从 X 到 X 的“移位”S, 它把序列 $(a_1, a_2, a_3, \cdots)$ 变为 $(0, a_1, a_2, a_3, \cdots)$(换言之, 它把一个 0 放在序列之首, 而把序列的其他元向右移一位). 映射 S 是线性的, 而如果 X 上的模不是太病态的话, S 还是从 X 到 X 的连续函数.

(ii) 如果 X 是定义在闭区间 $[0, 1]$ 上的函数空间[III.29], 而 w 是一个固定函数, 则把函数 f 映为乘积 fw(这是函数 $x\mapsto f(x)w(x)$ 的简写) 的映射 M 是线性的, 而当 w 在某个适当的意义下足够小的话, M 是从 X 到 X 的连续线性映射. 这种映射称为**乘子映射**(注意,“是一个乘子”这个性质, 不仅依赖于空间 X 和映射 M, 还依赖于把 X 表示为一函数空间的方式, 所以, 这个性质不是映射本身的内蕴性质).

(iii) 定义函数空间上的线性算子的另一个重要方法是利用所谓**核**. 核是一个两变元的函数, 用它来定义一个线性映射的方法, 有点像用矩阵来定义有限维向量空

间之间的线性映射. 下面的公式就利用了 K 来定义一个线性映射 T:

$$Tf(x)=\int K(x,y)f(y)\,\mathrm{d}y. \tag{1}$$

请注意它和下面的公式形式上的类似:

$$(Av)_i=\sum_j A_{ij}v_j,$$

后者定义了矩阵和列向量的乘积. 再说一下, K 需要满足适当的条件才能定义一个连续线性映射.

傅里叶变换 [III.27]$\mathcal{F}$ 用核来定义线性算子的好例子, $\mathcal{F}$ 把一个 $L^2(\mathbf{R})$ 的函数, 映为另一个 $L^2(\mathbf{R})$ 函数, 它是由下面的公式来定义的:

$$(\mathcal{F}f)(\alpha)=\int_{-\infty}^{\infty}f(x)\mathrm{e}^{-\mathrm{i}\alpha x}\mathrm{d}x,$$

这里的核就是函数 $K(\alpha,x)=\mathrm{e}^{-\mathrm{i}\alpha x}$.

(iv) 如果 f 是一个定义在例如 $\mathbf{R}$ 上的可微函数, 用 $\mathrm{D}f$ 来记它的导数, 可以把 D 看成一个线性映射, 因为 $\mathrm{D}(\lambda f+\mu g)=\lambda\mathrm{D}f+\mu\mathrm{D}g$. 为了能够把 D 看成一个算子, 需要 f 属于适当的函数空间. 做这件事的方法哪个算最好视问题的背景而异. 选择一个好的函数空间可以是重要的也是微妙的问题. 方法之一是不再坚持 D 必须定义在整个空间的每一个函数上, 也不要求 D 是连续的, 有时, D 虽然是不连续的, 但是定义在一个稠密的函数集合上也就够了.

类似地, 许多偏微分算子, 如**梯度**[I.3 §5.3] 和**拉普拉斯算子**[I.3 §5.4], 如果适当地看待, 都是线性算子.

2. 算子的代数

虽然个别的算子也可以是重要的, 但是若不是因为它们组成了**族**, 就不会像现在这样有趣. 如果 X 是一个巴拿赫空间, 则由 X 到其自身的连续线性算子的集合 $B(X)$ 形成一种结构, 称为**巴拿赫代数**. 粗略地说, 这句话的意思就是, $B(X)$ 不仅是巴拿赫空间 (其中的元、算子 T 的范数定义为 $\|Tx\|$ 在所有适合条件 $\|x\|\leqslant 1$ 的 x 之集合上的上确界, 亦即由下式定义: $\|T\|=\sup\limits_{\|x\|\leqslant 1}(\|Tx\|)$), 而且其中的元素既可以相加, 也可以相乘, 而且很容易证明这个乘积满足不等式 $\|T_1T_2\|\leqslant\|T_1\|\|T_2\|$. 当 X 是**希尔伯特空间**[III.37]H 时, 这个代数特别重要. $B(H)$ 的各个子代数有很丰富的结构, 见**算子代数**[IV.15].

3. 定义在希尔伯特空间上的算子的性质

希尔伯特空间 H 和一般的巴拿赫空间不一样, 其中有内积. 因此自然会要求把由 H 到 H 的连续线性算子与内积连接起来. 这个基本的思想引导到几个不同的定义, 其中的每一个都挑选出一个重要的算子类.

3.1 酉映射和正交映射

可能要求一个算子 T 的最自然的条件大概就是要求它保持内积, 就是说, 对于任意两个向量 x 和 y , $\langle Tx , Ty\rangle$ 应该等于 $\langle x , y\rangle$. 特别是这就蕴含了对于任意的向量 x, 都有 $\|Tx\| = \|x\|$. 所以, T 是一个等距映射 (即一个保持距离的映射). 如果进而还有 T 为可逆的 (当 T 的像是整个 H 时, 它自然是可逆的), 这时 T 就是一个**酉映射**. 酉映射构成一个群. 如果 H 是 n 维的, 这个群就是重要的*李群*[III.48 §1]$U(n)$. 如果 H 是一个实希尔伯特空间, 就要用"正交"这样的字眼来代替"酉"这个字眼, 而相应的李群就称为 $O(n)$. 当 $n = 3$ 时, 正交映射就是旋转和反射, 所以, 群 $O(n)$ 就是旋转和反射群对于 n 维的推广 ([所以, 上面讲到酉映射时, 应该设 H 是复希尔伯特空间]).

3.2 厄尔米特映射和自伴映射

给定任意由 H 到 H 的线性映射 T, 由下式可以定义另一个由 H 到 H 的线性映射 T^*: $\langle Tx , y\rangle = \langle x , T^*y\rangle$. 这个算子是唯一的, 并称为 T 的**伴算子**. T 可能具有的第二个性质就是与自己的伴算子相等, 即当且仅当对于每一对 x 和 y 都有下式成立: $\langle Tx, y\rangle = \langle x, Ty\rangle$. 对于一般的复的标量, 这种算子称为**厄尔米特算子**, 而当标量为实数时, 则称为**自伴算子**. 厄尔米特映射的一个简单来源是空间 $L^2[0 , 1]$ 上的乘子, 这时被用来乘空间 $L^2[0 , 1]$ 之元的函数是有界的实值函数, 马上就会看到在某种意义下, 这些是仅有的例子.

3.3 矩阵的性质

如果 H 是有限维的具有规范正交基底的空间, 则可以作出 T 相对于这个基底的矩阵 A. 上面讨论的 T 的种种性质就等价于这个矩阵 A 的性质. A 的**转置矩阵**A^{T} 是由式子 $\left(A^{\mathrm{T}}\right)_{ij} = A_{ji}$ 来定义的, 而其**共轭转置** A^* 则由 $(A^*)_{ij} = \bar{A}_{ji}$ 来定义. $n \times n$ 矩阵 A 是**酉矩阵**, 如果 $AA^* = I$ 是 n 阶单位矩阵; 是**正交矩阵**, 如果 A 是实矩阵, 而且 $AA^{\mathrm{T}} = I$; 是**厄尔米特矩阵**, 如果 $A = A^*$; 是**自伴矩阵**, 如果 $A = A^{\mathrm{T}}$(这时也说 A 是**对称矩阵**). 算子 T 具有以上四种性质之一, 如果矩阵 A 具有相应的性质.

3.4 谱定理

注意, 酉算子的伴算子就是它的逆. 由此可知, 酉算子和厄尔米特算子都与自

己的伴算子可换, 具有这个性质的算子称为正规算子. 正规算子由于谱定理而十分重要. 如果 T 是一个有限维空间 H 上的正规算子, 则谱定理断定 H 有一个由 T 的本征向量构成的*规范正交基底*[III.37]. 换言之, H 有一个由正交的单位向量构成的基底, 而相对于这个基底, T 的矩阵是对角矩阵. 在线性代数中, 这是一个极为有用的定理. 一般说来, 如果 T 是希尔伯特空间 H 上的正规算子, 谱定理告诉我们, H 也有一个类似于 "基底" 的东西, 而相对于它, T 是一个乘子. 稍微改变一下说法, 存在一个由 H 到由对于某个*测度*[III.55] 为平方可积的函数所成的希尔伯特空间

3.5 投影

希尔伯特空间上的另一类重要的映射是**正交投影**. 一般说来, 一个代数里的元素 T 称为**幂等的**, 如果它具有性质 $T^2 = T$. 如果这个代数是算子代数, 这种 T 就称为一个**投影**. 为了看清这个名词为什么很合适, 注意, 对于任意的空间 X, X 的每一个元素 x 都被 T 映到子空间 TX 里, 而已经在这个子空间里的元素都被 T 保持不动 (因为 $T(Tx) = T^2x = Tx$). [现在考虑 X 是希尔伯特空间 H 的情况]. 如果 Tx 恒正交于 $x - Tx$, 这个投影就称为**正交投影**. 这个概念告诉我们, T 是到 H 的一个子空间 Y 上的投影, 而把每一个向量都映到 Y 中最接近于它的向量, 这样, 向量 $x - Tx$ 就正交于整个子空间 Y.

III.51 数论中的局部与整体
(Local and Global in Number Theory)

Fernando Q. Gouvêa

类比是一个有力的工具. 当人们在两个不同的理论中看到了一种平行性, 就时常会把在一个理论中得到的洞察转移到另一个理论里去. "局部地" 研究一个对象这一思想来自函数理论, 利用函数和数的类比, 把这个思想引入数论, 就使我们得到了一种新的数, 即 p 进数, 还得到了**局部–整体原理**, 成为现代数论的指导思想之一.

1. 局部地研究函数

设有一个多项式例如

$$f(x) = -18 + 21x - 26x^2 + 22x^3 - 8x^4 + x^5.$$

即使是从函数的写法, 也马上能得到关于它的一些知识. 例如, 把 $x = 0$ 插入这个多项式, 就会得到 $f(0) = -18$. 其他一些事情就不那么明显. 例如为了决定 $f(2)$ 或 $f(3)$ 之值, 就需要做一点算术. 但是, 如果我们把这个多项式重新写为

$$f(x) = 5(x-2) - 6(x-2)^2 - 2(x-2)^3 + 2(x-2)^4 + (x-2)^5\ ,$$

就立刻可以看到 $f(2)=0$ (当然, 需要验证 $f(x)$ 的这两个表达式确实相等). 类似地, 可以验证

$$f(x)=10(x-3)^2+16(x-3)^3+7(x-3)^4+(x-3)^5,$$

而且立刻看到 $f(3)$ 也是 0, 事实上, 这个多项式在 $x=3$ 处有二重根.

思考这个问题的一个方法是说第一个表达式是 "局部在 $x=0$" 的表达式, 因为它对 $x=0$ 赋予了超乎其他值的地位. 于是, 另两个表达式就分别是局部在 $x=2$ 和局部在 $x=3$ 的表达式. 另一方面, 下面的表达式

$$f(x)=(x-2)(x-3)^2(x^2+1)$$

(它也是正确的) 就清楚地比较 "整体" 了. 它告诉我们根在哪里: 2, 3 和 $\pm\sqrt{-1}$, 其中 3 是二重根.

同样的方法可以推广到多项式以外的函数, 只要我们允许表达式是无限的. 例如取

$$g(x)=\frac{x^2-5x+2}{x^3-2x^2+2x-4},$$

"局部在 $x=0$", 可以把它写为

$$g(x)=-\frac{1}{2}+x+\frac{1}{2}x^2-\frac{3}{8}x^3-\frac{3}{16}x^4+\frac{7}{32}x^5+\cdots,$$

或者 "局部在 $x=2$", 有

$$g(x)=-\frac{2}{3}(x-2)^{-1}+\frac{5}{18}+\frac{5}{54}(x-2)-\frac{35}{324}(x-2)^2+\frac{55}{972}(x-2)^3$$
$$-\frac{115}{5832}(x-2)^4+\frac{65}{17496}(x-2)^5+\cdots.$$

注意, 这一次使用了 $x-2$ 的负幂, 因为在把 $x=2$ 插入时分母为 0. 但是这个表达式告诉我们, $x=2$ 的 "坏" 也不太过分. 具体说来, $g(2)$ 虽然无定义, $(x-2)g(x)$[在 $x=2$ 时] 仍有意义, 而且就是 $-\frac{2}{3}$.

继续往下走也很容易. 要想 "局部在 a" 掌握一般的函数, 有时还会需要用 $(x-a)$ 的分数幂, 但是这也不算太坏, 这种表达式在函数论中是有力的工具. 发现 p 进数的动机之一, 就是想在研究数的时候也有一个类似的有力工具.

2. 数也像函数

首先认识到可以在数和函数中找到这种类比的人是戴德金[VI.50] 和韦伯

(Heinrich Weber)①. 在他们的框架里, 正整数比作多项式, 分数则比作多项式之商, 例如, 上面的 $g(x)$. 更复杂的数则比作更复杂的函数类, 例如, 椭圆函数[V.31] 比作某一类代数数. 另外, 像 $\sin x$ 这样的函数, 就更像超越数如 e 和 π.

为了更好地了解函数, 戴德金和韦伯推进了 "函数像是数" 这样的思想. 特别是他们证明了为研究代数数而发展起来的一套技巧, 可以用来研究一类函数, 这一类函数后来就称为代数函数. 然而是亨泽尔 (Kurt Hensel, 1861–1941, 德国数学家) 看到, 如果说函数像是数, 那么数也像函数. 特别是, 他进而去寻找一个在函数论中如此有用的局部展开式在数论领域中的类比.

为了达到亨泽尔的思想, 我们首先要注意到, 通常表示数的方法已经指出了正确的方向. 说到底, 例如, 34 291 实际上是指

$$34291 = 1 + 9 \cdot 10 + 2 \cdot 10^2 + 4 \cdot 10^3 + 3 \cdot 10^4 .$$

如果我们允许把 10 看作是某个像是变量 x 的东西, 这个数的表达式恰好就是一个多项式. 更进一步, 如同可以把一个多项式按照不同的 $(x-a)$ 来展开一样, 也可以把同一个数按照不同的底来展开, 例如

$$34291 = 4 + 4 \cdot 11 + 8 \cdot 11^2 + 3 \cdot 11^3 + 2 \cdot 11^4 .$$

很容易看出这个展开式是怎样得出的. 先用 11 去除 34291, 得到余数为 4. 其次, 从原数减去 4 得到一个可以用 11 整除的数:

$$34291 - 4 = 34287 = 3117 \cdot 11.$$

现在再用 11 除 3117 得出第二个余数也是 4, 就是展开式中的第二项 "系数". 继续这样做下去, 就得到以 11 为底的展开式.

看起来这样做很能解决问题, 但是这里遗漏了一小点洞察. 事实是, 10 并不真像 $x-2$, 因为 10 **可以分解因子**而 $(x-2)$ 不行. 所以, 把一个数以 10 为底展开, 有点像把一个多项式展开为 (x^2-3x+2) 的幂, 而后者又可以分解为因子 $(x-2)(x-1)$. 这样的展开并不真是局部的, 因为它同时在看 x 的两个可能的值. 类似地, 以 10 为底的展开式既包含了一个数相对于 2 的信息, 也包含了它相对于 5 的信息. 结果是, 我们应该用**素数**为底.

以 11 为底只是为了说话确定一点. 我们已经知道, 可以把一个整数用 11 为底写出来, 也就是写成 "11 的各次幂的多项式". 用分数来试一下如何? 取 $\frac{1}{2}$ 为例. 第一步是找余数, 就是要在 0 与 10 之间找一个数 r, 使 $\frac{1}{2} - r$ 可以用 11 整除. 好,

---

① 19 世纪的数学史上有好几位韦伯. 最年长的一位是 Wilhelm Edouard Weber, 1804–1891, 他是物理学家, 高斯在电磁理论方面的著名合作者; 这一位全名是 Heinrich Martin Weber, 1842–1913, 来自哥尼斯堡, 主要的贡献在代数、数论以及函数论及其应用. —— 中译本注

$\frac{1}{2}-6=-\frac{11}{2}=-\frac{1}{2}\cdot 11$ 就行, 因此展开式的第一项是 6(为了弄明白现在 "整除" 是什么意思, 看一下如果取 $r=4$ 会发生什么情况. 这时, $\frac{1}{2}-r$ 将是 $-\frac{7}{2}$, 如果用 11 去除它, 将会得到 $-\frac{7}{22}$. 这时分母将以 11 为因子, 而这是不许可的, 在 $r=6$ 时也不会发生这个情况).

现在对 "商" $-\frac{1}{2}$ 再做同样的事. 我们看到 $-\frac{1}{2}-5=-\frac{11}{2}=-\frac{1}{2}\cdot 11$, 所以展开式的第二项是 $5\cdot 11$. 但是再往下做就又一次遇到了 $-\frac{1}{2}$! 所以我们就会这样无尽地做下去, 以后各项的系数全是 5. 换言之,

$$\frac{1}{2}=6+5\cdot 11+5\cdot 11^2+5\cdot 11^3+5\cdot 11^4+5\cdot 11^5+\cdots.$$

这时, 等号 "=" 是什么意思还不太明白. 但无论如何, 我们得到了一个 11 的幂所成的无限展开式, 称为 $\frac{1}{2}$ 的 **11 进展开式**. 此外, 在做算术时, 这个展开式还 "管用". 例如, 用 2 去乘它, 并把结果重新排列 ($2\times 6=12=1+11$, 后一个 11 用于进位等等), 最后得到的还是 1 $\left(=2\times\frac{1}{2}\right)$.

亨泽尔证明了只要许可无限展开式, 而且许可其中有有限多个 11 的负幂, 有时还有 11 的分数幂, 则对于所有的代数数就都能这样做 (所以, 可以处理 $\frac{5}{33}$和类似的东西). 他争辩说, 这就给出了 "局部在 11" 的信息. 对于所有的素数 p 都有这样的事情. 所以, 如果有素数 p, 就能 "局部在 p" 考虑一个数, 只要取这个数的 p 的幂的展开式即可. 而这个展开式就称为此数的 ***p* 进展开式**. 和在函数的情况类似, p 进展开式告诉我们这个数在多大程度上可以用 p 整除, 但是把此数关于其他的素数的情况都隐藏起来了, 在这个意义下, 它是真正 "局部的".

3. p 进数

最好的答案总是会提出新问题. 既已发现了任意的有理数都有 p 进展开式, 而且可以用来直接 "做算术", 就不可避免地会问, 这样做是否已经扩大了所考虑的数的世界. 一旦选定了一个素数 p, 则任意有理数就给了一个 p 进展开, 但是是否每一个这样的展开都是来自一个有理数?

毫无可能. 容易看到, 这种展开式的集合远大于所有有理数的集合. 所以亨泽尔的下一步棋, 就是指出所有 p 进展开式的集合 $\mathbf{Q}_p$ 是一个新的数的领域, 他把这些数称为 ***p* 进数**, 其中不仅有有理数, 还有更多的东西.

考虑 $\mathbf{Q}_p$ 的最佳办法就是拿它来和所有实数的集合 $\mathbf{R}$ 作类比. 实数通常是用十进展开式来表示的. 当写出 $\mathrm{e}=2.718\cdots$ 时, 就是指

$$\mathrm{e}=2+7\cdot 10^{-1}+1\cdot 10^{-2}+8\cdot 10^{-3}+\cdots.$$

所有这种展开式的集合就是所有实数集合, 其中包括有理数, 但是要大得多.

当然, 除了都包含有理数以外, 这两个领域几乎完全不同. 例如, 在 $\mathbf{Q}_p$ 和 $\mathbf{R}$ 中, 都有 "两个数的距离" 这个自然的概念. 但是这两种距离完全不同, 哪怕所涉及的数是有理数也是如此. 例如, 在实数域里, 2 和 2001/1000 非常接近, 但是例如在 5 进数域里二者的距离就很大!

因此, 可以用 p 进数作计算, 和用实数作计算一样. 许多其他的数学概念也可以推广. 所以, 亨泽尔的思想引导到 "平行的 (数的) 宇宙" 的系统 —— 对每一个素数有一个宇宙, 还要加上实数的宇宙 —— 而可以在其中 "做数学".

4. 局部–整体原理

一开始, 绝大多数数学家们似乎觉得亨泽尔的新数有形式的兴趣, 但是也怀疑其要点何在. 人们接受一个新数不是为了好玩, 它需要对于做某件事有用. 亨泽尔为自己的新数着了迷, 他写了一篇又一篇文章, 但是一开头, 对于证明它们是有用的, 他确实遇到了麻烦. 例如, 他证明了可以用它们以一种新的方式来发展代数数论的基础 —— 但是绝大多数人还是喜欢老办法.

可以通过对于一个困难的结果给出一个漂亮而且初等的证明来表明一个新思想的力量, 亨泽尔写了一篇论文来做这样的事情. 他对于 e 为超越数, 给出了一个容易而且漂亮的 p 进证明. 这一点确实引起了人们的关注. 不幸的是, 当人们仔细地考察这个证明时, 发现了其中有微妙的错误, 结果是数学家对于亨泽尔的奇怪的新数的怀疑反而加强了.

这个潮流由于哈塞 (Hermut Hasse, 1898–1979, 德国数学家) 的工作而得到改变. 哈塞曾经在哥廷根读书, 有一次, 他漫步走进了一家书店, 找到一本书, 即后面文献目录里的 (Hensed, 1913), 这是前几年才出版的一本书. 哈塞为之着迷, 就到 Marburg 去跟亨泽尔读书. 1920 年, 就是几年以后, 他找到了一个思想, 使得 p 进数成了数论家们的关键工具.

哈塞所证明的是数论里的一些问题可以通过 "局部地" 回答来解决, 下面是一个例子 (虽然不甚重要, 却相当好懂). 设 x 是一个有理数, 而且是另一个有理数 y 的平方, 所以 $x = y^2$. 因为所有的有理数都是 p 进数, 所以**对于任意的素数 p, 数 x 看成一个 p 进数, 都是一个平方**. 类似地, 实数 x 也是一个平方, 所以有理数 y 就是一个 "整体的" 平方根, 即在每一个局部背景下都是平方根.

至此为止, 一切都很乏味. 但是现在把问题反过来看. 假设已知**对于任意的素数 p , 数 x 看成一个 p 进数, 是某个 p 进数 (可能依赖于 p) 的平方,** 又设 x 看成一个实数时是某个实数的平方. 先验地看, x 的这些局部平方根都可能是不同的! 但是在这些假设下, x 必须是**某个有理数**的平方, 因此所有的局部根必定都来自一个 "整体" 根.

这就引导我们把有理数看成"整体的", 而把不同的 $\mathbf{Q}_p$ 和 $\mathbf{R}$ 看成是"局部的". 这样一来, 前面这段话指出了"是一个平方"这个性质, 当且仅当它"处处局部地"为真时, 才整体为真. 这是一个很有力又很有启发的思想, 后来就以"**哈塞原理**"或者"**局部–整体原理**"之名而著称于世.

我们的例子当然只是在最强的情况下证明了这个原理, 在所有情况下局部地解决了一个问题, 也就整体地解决了这个问题. 在所有情况下局部地解决问题, 当然时常是过高的期望. 然而, 局部地攻击一个问题, 再把局部的结果放在一起, 这是现代数论的一个基本技巧. 它已经被用来简化老的证明, 例如, 在类域理论[V.28] 中; 也被用来得出新证明, 怀尔斯在费马大定理的证明 [V.10] 中就是这样做的. 所以, 亨泽尔还是对的, 在数论家的心目中, 他的新数已经得到了和实数同等的地位.

进一步阅读的文献

Gouvêa F Q. 2003. *p-adic Numbers: An Introduction*, revised 3rd printing of the 2nd edn. New York: Springer.

Hasse H. 1962. Kurt Hensels entscheidener Anstoss zur Entdeckung des Lokal-Global-Prinzips. *Journal für die reine und angewandte Mathematik*, 209:3-4.

Hensel K. 1913. *Zahlentheorie.* Leipzig: G. J. Göschenische.

Roquette P. 2002. History of Valuation, I, In *Valuation Theory and Its Applications.* Providence, RI: American Mathematical Society, I:291-335.

Ullrich P. 1995. On the origins of p-adic analysis. *Proceedings of the 2nd Gauss Symposium. Conference A: Mathematics and Theoretical Physics*, Munich, 1993: 459-73. Symposia Gaussiana. Berlin: Walter de Gruiter.

Ullrich P. 1998. The genesis of Hensel's p-adic numbers. In *Charlemagne and His Heritage: 1200 Years of Civilization and Science in Europe.* Turnout:Brepols, 2:163-78

对数函数

(The Logarithmic Function)

见指数和对数函数 [III.25]

III.52 芒德布罗集合

(The Mandelbrot Set)

设有一个复多项式 $f(z) = z^2 + C$, 其中 C 是一个复常数. 这时, 任意选一个复数 z_0 作为初值, 并且用此公式作迭代, 即可得序列 $z_0, z_1, z_2, \cdots$. 也就是令

$z_1 = f(z_0)$, $z_2 = f(z_1)$ 等等. 有时这个序列会趋向无穷, 有时又会保持有界, 即与 $z = 0$ 的距离在一定限度之内. 例如, 取 $C = 2$, 并从 $z_0 = 1$ 开始, 这个序列将是 $1, 3, 11, 123, 15131, \cdots$, 显然趋于无穷. 但是, 如果从 $z_0 = \frac{1}{2}(1 - i\sqrt{7})$ 开始, 则将有 $z_1 = z_0^2 + 2 = z_0$. 这个序列当然是有界的, 因为它的各项都等于 z_0. 与此常数 C 相关的**茹利亚**(Gaston Maurice Julia, 1893–1978, 法国数学家)**集合**就是使得这个序列保持有界的 z_0 的集合. 茹利亚集合常有分形的形状 (见 [IV.14§2.5]).

在定义茹利亚集合时, 我们是固定 C 并且考虑 z_0 的各种可能性的. 如果固定 z_0 并且考虑 C 的各种可能性又如何? 结果就是**芒德布罗**(Benoit Mandelbrot, 1924–2010, 生于波兰后入籍美国的法国数学家) 集合. 它的确切的定义是: 取 $z_0 = 0$, 一切使上述序列有界的复数 C 的集合就是芒德布罗集合 (当然可以考虑其他的 z_0, 但是结果并没有有意义的区别, 因为它们之间有一个简单的变量变换关系).

芒德布罗集合也有错综复杂的结构, 而且俘获了广大民众的想象力. 芒德布罗集合的详尽的几何构造至今还未完全了解, 由此产生的一些未解决问题有很大的重要性, 因为其中隐藏了关于动力系统的很一般的信息, 详见*动力学*[IV.14 §2.8].

III.53 流 形 (Manifolds)

球面有如下的性质: 如果只看它的很小的一部分, 这一部分看起来就和平面的一部分一样. 比较一般地说, 一个 ***d* 维流形**, 也叫 ***d* 流形**, 就是一个 "局部地" 和 d 维*欧几里得空间*[I.3 §6.2] 一样的几何对象. 这样, 2 流形就是一个光滑曲面, 例如球面或者环面. 高维流形比较难 "看见", 但是是一个重大的研究课题. 我们在条目*某些基本的数学定义*[I.3 §6.9, 6.10] 里开始讲到它, 关于它更高深的思想在*微分拓扑*[IV.7] 和*代数拓扑*[IV.6] 里面讨论, 还可以参看*代数几何*[IV.4]、*模空间*[IV.8] 和*里奇流*[III.78] 等条目 (这远不是讲到流形的条目完备的清单).

III.54 拟 阵 (Matroids)

Domonic Welsh

惠特尼 (Hassler Whitney , 1907–1989, 美国数学家)1935 年提出拟阵概念的原来的目的是想给出一个抽象的代数概念, 以包括*向量空间*[I.3 §2.3] 中向量的集合结构的主要成分, 而又避免明显地提到线性相关.

为此, 他把向量空间的两个基本性质分离出来, 并且规定, 任意具有这两个性质的子集合的族都是一个 “拟阵” 的 “独立集合” 的集合. 第一个性质是明显的: 线性无关集合的子集合也是线性无关的. 第二个性质就比较微妙了: 如果 A 和 B 是两个线性无关集合, 而 B 中的元素比 A 中的元素多, 则在 B 中一定存在不属于 A 的元素, 但若把它添加到 A 中, 仍然给出一个线性无关集合. 为了避免平凡不足道的情况, 他最后还坚持, 在任意一个拟阵中, 空集合必须是独立的.

这样, 一个**拟阵**形式上看就是一个有限集合 E, 其中规定了 E 的某些子集合称为**独立集合**, 它们要满足下面的公理:

(i) 空集合是独立集合.

(ii) 独立集合的任意子集合仍是独立集合.

(iii) 若 A 和 B 都是独立集合, 而 A 中元素的个数比 B 中元素的个数少 1, 这时, B 中必有不在 A 中的元素 x, 使得 $A\cup\{x\}$ 仍是独立集合.

性质 (iii) 称为**交换公理**. 拟阵的最基本的例子就是向量空间的向量之集合, 而 “独立集合” 则是通常的线性无关集合. 在这个情况下, 交换公理就是 Steinitz 交换引理. 然而, 真的有许多并非向量空间的子集合的例子.

下面的例子是来自图论的一个重要的拟阵类. 图中的一个循环就是下面形式的边的集合: (v_1, v_2), (v_2, v_3), $\cdots$, (v_{k-1}, v_k), (v_k, v_1), 其中所有的顶点 v_i 都是彼此不同的. 任取一个图, 并且把其中不包含循环的边的子集合称为 “独立集合”.

这样, 这里是把循环看成有点像是向量之间的线性相关. [公理 (i) 的成立是自明的]; 至于公理 (ii), 很明显, 一个独立集合的子集合一定也是独立集合, 所以 (ii) 也是满足的. 稍微不那么明显的是 (iii), 如果 A 和 B 分别有 t 个和 $t+1$ 个边, 二者都不包含循环, 则 B 中至少有一条边不在 A 中, 但是若把这条边添加到 A 中, 也不会造成一个循环. 这样就又看到一个拟阵, 而且出现在与向量空间很不相同的背景下.

但是, 有一个方法能把图的边与 $\mathbf{F}_2$ 上的向量空间的向量集合等同起来, 这里 $\mathbf{F}_2$ 是整数 mod 2 所成的域 (见*模算术*[III.58]). 如果一个图 G 有 n 个顶点, 作 n 维向量空间 $\mathbf{F}_2^n$, 取其一个基底, 其中必有 n 个 $\mathbf{F}_2^n$ 向量, 对 G 的每一个顶点都附加上此基底的一个向量. 对于 G 的每一个边都可以附加上相应于其两个端点的基底向量的和所成的向量, 于是边的一个集合是独立集合当且仅当相应的 $\mathbf{F}_2^n$ 向量集合是线性无关的. 然而, 我们将会看到, 有重要的拟阵的例子, 甚至不能**同构于**向量的集合.

要注意, (一个图的) 独立集合之集, 只能传递图的部分信息, 而绝非全部信息. 例如, 考虑图 1 中的图 G 和 H. 作为图, 它们是不同的, 但是它们给出了集合 $\{a, b, c, d\}$ 上的同样的拟阵 (其独立集合就是大小小于或等于 3 的子集合, 但是

要除去 $\{a, b, c\}$). 注意, 这个拟阵和下面的矩阵的各列所成的拟阵是相同的：

$$A = \begin{array}{c} \begin{matrix} a & b & c & d \end{matrix} \\ \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \end{array}.$$

然而, 绝大部分拟阵并非来自图或矩阵.

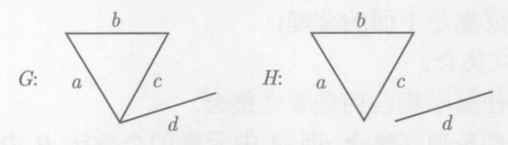


图 1　两个给出同样拟阵的图

拟阵虽然是由很简单的公理定义的, 但是许多线性代数和图论的结果都可以推广到更广的拟阵的背景下. 例如, 设 G 是一个连通图, 如果 B 是 G 上拟阵的最大独立集合, 则 B 是一个与 G 的所有顶点连接的树, 称为 G 的**张树**(spanning tree). 一个连通图的所有张树都有相同的边数, 即比顶点数少 1. 类似地, 在一个向量空间中, 确切一点说, 在向量的任意子集合中, 所有最大的线性无关集合大小均相同. 这两个结果都是关于拟阵的一般结果的特例. 这个一般结果就是：在任意拟阵中, 所有最大独立集合大小均相同. 这个公共的大小称为拟阵的**秩**, 而与向量空间作类比, 所有最大独立集合都称为其**基底**.

拟阵自然地出现在数学的许多部分里, 而且其出现时常是很突然的. 例如, 考虑**最小联络问题**：一个公司需要有连线接通到一些城市, 例如用铁路或者电话电缆, 而且希望能使总成本最小. 这就等价于以下问题：给定一个连通的图 G, 对其每一边 e 都赋有一个权重 $w(e)$, 求边的一个集合, 使能连接 G 的所有顶点, 但是总权重最小. 不难看到这个问题可以化为求具有最小权重的张树的问题.

这个问题有一个经典的算法. 它是可能想到的可能最简单的算法, 它是这样做的. 从选取权重最小的边开始, 下面的每一步都对所选取的集合加一个权重最小的边, 而又不要形成循环.

例如考虑图 2. 按照这个算法应该依次选取以下各边：(a, b), (b, c), (d, f), (e, f), (c, d), 这样得到一个总权重为 $1+2+3+5+7=18$. 由于这个算法是这样工作的, 所以称为贪婪算法.

初看起来这个算法很不像是能够管用, 因为它否定了选取次佳的边的可能性, 以后这就可能要付出代价. 然而, 不难证明, 它是正确的. 事实上, 它几乎可以完全相同地推广到一般的拟阵：它所给出的实际上是一个 (相当快的) 在各个元都带有非负权重的拟阵中选取具有最小总权重的基底的算法.

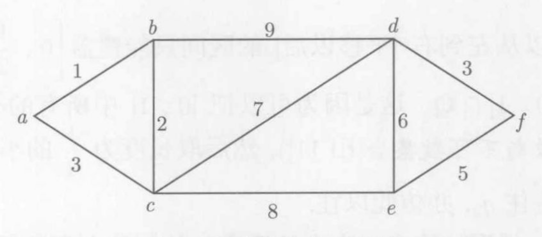


图 2　各边带有权重的图

更惊人的是拟阵是贪婪算法能够管用的唯一的结构. 更精确地说, 设 $\mathcal{I}$ 是一个集合 E 的一个子集合族, 而且具有以下的性质: 若 $A \in \mathcal{I}$ 而 $B \subseteq A$, 则 $B \in \mathcal{I}$. 设 w 是任意权函数, 而问题是选取 $\mathcal{I}$ 的一个具有最大权重元素 $B \in \mathcal{I}$, 而所谓一个集合的权重就是其中各个元素权重的和. 和上面一样, 贪婪算法从选取具有最大权重的元素 e 开始, 然后再从余下的元素中选取具有最大权重的元素, 但要服从一个附带要求, 就是在任何阶段, 选出的元素构成一个属于 $\mathcal{I}$ 的子集合. 因此, 以下事实为真: **当且仅当 $\mathcal{I}$ 是一个拟阵的所有独立集合的集合时, 贪婪算法在赋有任意权重函数的 $\mathcal{I}$ 上管用**. 这样, 拟阵成了许多优化问题的 "自然的家". 此外, 拟阵这个概念是真正有用的, 因为许多出现在这种问题中的拟阵都不是从向量空间或从图导出的.

III.55 测　度
(Measures)

为了懂得测度理论, 明白它为什么有用和重要, 从关于长度的问题开始是有益的. 设在区间 $[0, 1]$(从 0 到 1 的闭区间) 内有一串区间, 其总长度小于 1, 问它们能否覆盖 $[0, 1]$? 换言之, 设给定区间 $[a_1, b_1], [a_2, b_2], \cdots$, 而且 $\sum(b_n - a_n) < 1$, 它们的并能否等于 $[0, 1]$?

人们会想说 "不行, 因为总长度太小". 但这只是把问题换了一个说法. 毕竟, 为什么 "总长度小于 1" 确实蕴含了这些区间不能覆盖 $[0, 1]$? 另外有人可能想说 "把这些区间从左到右重新排列, 绝不能达到 $[0, 1]$ 的右端". 换句话说, 如果第 n 个区间 $[a_n, b_n]$ 的长度是 d_n, 则可以把这些区间平移为 $[0, d_1], [d_1, d_1 + d_2], \cdots$. 在这样重排以后, 确实不能覆盖 $\sum d_n$ 以外的点, 但是, 为什么这就意味着原来的区间不能覆盖 $[0, 1]$ 呢?

很容易看到, 在**有限个**区间的情况, 这种重排的论据是可以用的, 但是在一般的情况就不行. 事实上, 如果再问原来的问题, 但是把 $[0, 1]$ 换成其中的有理数的集合 $[0, 1] \cap \mathbf{Q}$. 如果 $[a_1, b_1], [a_2, b_2], \cdots$ 这些区间的长度分别是 $\frac{1}{4}, \frac{1}{8}, \frac{1}{16}, \cdots$,

其总长度是 $\frac{1}{2}$, 所以从左到右 [平移以后] 的区间只能覆盖 $\left[0\,,\,\frac{1}{2}\right]\cap\mathbf{Q}$, 但是, 原来的区间可以覆盖 $[0\,,\,1]\cap\mathbf{Q}$. 这是因为可以把 $[0\,,\,1]$ 中所有的有理数排列为序列 $q_1\,,\,q_2\,,\cdots$ (**见可数与不可数集合**[III.11]), 然后取长度为 $\frac{1}{4}$ 的小区间盖住 q_1, 取长度为 $\frac{1}{8}$ 的小区间盖住 q_2, 并仿此以往.

这一点就说明, 问题的答案一定会涉及实数的一些有理数所不具有的性质, 正是这些性质使得那些 "明显可见" 之类的话垮了台. 其实, 说这些区间不能覆盖 $[0\,,\,1]$, 这个结果是对的, 但是去证明它是一个好练习.

为什么这是一件重要的事实? 这是源于想要对一般实数集合定义其 "长度"(为简单计, 我们集中讨论 $[0\,,\,1]$, 以避免关于 "无限长度" 这样的技术细节). 一个集合的 "长度" 应该是什么? 对于一个区间, 答案是明显的. 对于区间的有限并, 也是清楚的. 但是, 关于像 $\left\{\frac{1}{2}\,,\,\frac{1}{3}\,,\,\frac{1}{4}\,,\cdots\right\}$ 这样的集合以至于 $\mathbf{Q}$ 本身, 又该怎么说?

一个自然的初步的企图是使用区间的有限并: 可以规定集合 A 的长度, 就是所有的覆盖 A 的有限个区间的长度的最小值. 精确一点说, 可以定义 A 的长度为 $(b_1-a_1)+(b_2-a_2)+\cdots$ 的下确界, 这里的下确界是对于所有使得 $[a_1\,,\,b_1]\cup[a_2\,,\,b_2]\cup\cdots$ 能够覆盖 A 的有限个区间的并来取的.

不幸的是, 这个定义有一些我们不愿见到的性质. 例如, 区间 $[0\,,\,1]$ 中的所有有理数的集合长度, 按照这个定义, 应该为 1; $[0\,,\,1]$ 中所有无理数的集合的长度也应该为 1. 这样就会有两个互相分离的集合 (而且是非常自然的集合), 其并的长度不等于这两个集合的长度之和. 所以, 对于这种集合, 这样的 "长度" 不能算是功能良好的.

我们需要的是这样一个 "长度" 的概念, 它要能用于所有我们知道的习惯的集合, 而且要是可加的, 就是说, 只要 A 和 B 是分离的集合, 则 $A\cup B$ 的长度应该是 A 的长度和 B 的长度之和. 值得注意的是, 这是可以做到的, 而关键在于只要取**可数覆盖**就能做到这一点. 就是说要把长度的定义修改如下: 集合 A 的长度 (通用的术语是测度) 是区间 $[a_n\,,\,b_n]$ 的长度之和 $(b_1-a_1)+(b_2-a_2)+\cdots$ 的下确界, 这里的下确界是对于所有使得 $[a_1\,,\,b_1]\cup[a_2\,,\,b_2]\cup\cdots$ 能够覆盖 A 的 [最多可数个] 区间的并来取的. 注意, 对于前面所讨论过的 "悖论", 现在可以看到, 区间 $[a\,,\,b]$ 的测度确实是 $b-a$, 而这正是我们希望见到的.

现在不难证明 $[0\,,\,1]$ 中的所有有理数的集合的测度为 0, 而 $[0\,,\,1]$ 中的无理数集合的测度为 1. 实际上, 所有的可数集合的测度都是 0. 在许多情况下, 测度为 0 的集合是可以 "忽略的" 或者说是 "不重要" 的. 值得提一下, 也有不可数的零测度集合 (**康托集**[III.17] 就是一个例子).

以后会看到, 即令使用了这样的测度定义, 也还能找到这样一对互相分离的集

合 A 和 B, 使得 $A \cup B$ 的测度不等于 A 的测度和 B 的测度之和. 然而可以证明, 对于所有 "合理的" 集合, 测度是可加的. 准确一点的说法是, 我们说 $[0, 1]$ 的子集合是一个**可测集合**, 如果它和它的余集合的测度之和为 1, 而它们应该是这样的. 如果 A 和 B 是互相分离的可测集合, 则它们的并 [也是可测集合], 而且其测度等于它们各自的测度之和.

这是一个很有用的事实. 因为数学中自然出现的集合或者有显式定义的集合 [几乎] 都是可测集合, 区间、区间的有限并、区间的可数并、康托集、所有涉及有理数和无理数的集合 [几乎] 都是可测集合. 事实上, 可数多个可测集合的并仍是可测集合, 这件事实我们就说成是: 可测集合构成一个 **σ 代数**. 还有更好的事: 对于可测集合, 测度是**可数可加的**, 意思是可数多个互相分离的可测集合的并 [仍是可测集合, 而且] 其测度是各个集合独自的测度之和.

一般说来, 在许多其他的背景下, 也总想找到一个 σ 代数, 而把我们所关心的集合全都包含在内, 而在这个 σ 代数上, 就可以定义一个可数可加测度, 或者说是 "长度函数". 上面的例子就叫做 $[0, 1]$ 上的**勒贝格测度**. 一般说来, 当我们想定义一个可数可加测度时, 总要从上面提出的那个 "悖论" 入手.

所有**波莱尔集合**(Borel set) 构成一个重要的 σ 代数. 这是包含所有开区间和闭区间的最小的 σ 代数, 粗略地说, 波莱尔集合就是从开的和闭的区间用可数并和可数交所能够做出来的所有的集合 (但是这样说掩盖了一件事实, 即这个构造的过程可以是极端复杂的: 在波莱尔集合中存在超限的层次 (hierarchy)). 波莱尔集合的 σ 代数小于勒贝格可测集合的 σ 代数, 因为一个任意的零测度集合不一定是波莱尔集合. 波莱尔集合是描述集合论[IV.22§9] 的基本概念之一, 在某种技术性的意义下, 它们是 "容易描述的".

下面是具有可数可加测度的 σ 代数的另一个例子, 可以在 $[0, 1]^2$(即平面上的单位正方形) 上来构造它, 而以矩形而非区间为基础. 这样, 就定义一个集合的测度为一串覆盖此集合的矩形的并的最小面积, 这给出处理积分的漂亮而且有力的途径: 一个函数 (例如, 是定义在 $[0, 1]$ 上, 也在 $[0, 1]$ 上取值的函数) 的积分就定义为其 "图像下方的面积", 即集合 $\{(x, y) : 0 \leqslant y \leqslant f(x)\}$ 的测度. 许多看起来很复杂的函数现在可以积分了, 例如, 在有理点上取值 1, 而在无理点是取值 0 的函数, 就很容易检验是可积分的, 而且其积分为 0, 而在较早的积分理论, 例如黎曼积分理论中, 它的变化过于急速所以不能积分.

这种处理积分的途径产生出**勒贝格积分**(进一步的讨论可以见于条目勒贝格[VI.72]), 它是数学的基本概念之一. 它使我们能够积分很广的一类函数, 而这些函数不是黎曼可积的. 然而它的重要性的理由并不在此, 而在于勒贝格积分有很好的而黎曼积分所没有的极限性质. 例如, 设 $f_1, f_2, \cdots$ 是一个从 $[0, 1]$ 到 $[0, 1]$ 的勒贝格可积函数的序列, 而且对于每一点 x, $f_n(x)$ 都收敛于 $f(x)$. 这

时, f 必定也是勒贝格可积的, 而且函数 f_n 的勒贝格积分必收敛于 f 的勒贝格积分.

III.56 度量空间
(Metric Spaces)

在数学中, 特别是在分析中, 在许多情况下, 我们想说两个数学对象是接近的, 并且能精确地理解这句话的意思. 如果这两个对象是平面上的点 (x_1, x_2) 和 (y_1, y_2), 这个任务是直截了当的, 根据毕达哥拉斯定理, 它们之间的距离就是

$$\sqrt{(y_1-x_1)^2+(y_2-x_2)^2}.$$

说这两个点很接近也是有意义的, 即两个点的距离很小.

现在设有 n 维空间中的两个点 $(x_1, \cdots, x_n)$ 和 $(y_1, \cdots, y_n)$. 推广上面 $n=2$ 时的结果是一件简单的事, 于是定义它们之间的距离是

$$\sqrt{(y_1-x_1)^2+(y_2-x_2)^2+\cdots+(y_n-x_n)^2}.$$

当然, 只是这个公式容易推广这一点, 还不足以说明这个公式是距离的合理的定义. 这就提出了一个问题: 我们希望具有哪些性质才是合理的定义呢？度量空间就是来自这种思考的抽象的概念.

令 X 是一些"点"的集合. 设给定了两个这样的点, 例如是 x 和 y, 而且我们有方法指定一个实数 $d(x, y)$, 而我们愿意以之为这两点的距离. 下面三个性质就是我们非常希望距离的概念所具有的:

(P1) $d(x, y)\geqslant 0$, 而且等号成立当且仅当 $x=y$.

(P2) 对于任意两点 x 和 y, $d(x, y)=d(y, x)$.

(P3) 对于任意三点 x, y 和 z, $d(x, y)+d(y, z)\geqslant d(x, z)$.

三个性质的第一条说明两点的距离一定是正的, 除非这两点重合, 此时距离就是 0. 第二条说明距离是一个**对称**的概念: 从 x 到 y 的距离和从 y 到 x 的距离是一样的. 第三条称为**三角形不等式**: 如果把 x, y 和 z 想象为一个三角形的顶点, 则任意一边的长度不会超过另两边的长度之和.

对于集合 X 的一对点 (x, y) 定义的函数 $d(x, y)$, 如果满足条件 (P1) 到 (P3), 就称为 X 上的一个**度量**. 这时, X 加上 d 就叫做一个**度量空间**. 通常的距离概念的这种抽象化是很有用的. 度量有许多重要的例子不一定是从毕达哥拉斯定理导出的, 下面是几个例子.

(i) 令 X 为一个 n 维空间, 即由 n 个实数所成的序列 $(x_1, \cdots, x_n)$ 的集合 $\mathbf{R}^n$. 可以证明, 上面由毕达哥拉斯定理导出的公式给出了一个恰好具有性质 (P1)

到 (P3) 的度量. 这个度量称为**欧几里得距离**, 所得到的空间就叫做**欧几里得空间**. 它在数学里可能是独有的最基本最重要的一类度量空间.

(ii) 近年来, 所有的信息都是以 000111010010 这样形式的一连串 0 和 1 数字地传输的. 两个这样的数字串的汉明 (Hamming) 距离就等于这两个串中数码不同的位置的个数, 例如, 00110100 和 00100101 的汉明距离就是 2, 因为这两串数码只有第 4 位和第 8 位不同. 这个距离概念也满足 (P1) 到 (P3)

(iii) 如果驾车从一个城市到另一个城市去, 所关心的并不是乌鸦飞过了多少距离, 而是在可以走的道路网络中的最短距离. 类似地, 如果您想从伦敦到悉尼去, 那么关乎重要的是地球表面上的最短路径 (称为**测地线**) 的长度, 而不是穿到地球里面去的 "真正的" 距离. 许多有用的度量都是来自这个最短路径的一般概念. 它能保证 (P3) 成立.

(iv) 欧几里得距离的一个重要的特点是它的旋转对称性, 换句话说, 对平面或者空间作一个旋转, 并不会改变两点的距离. 还有其他的度量具有许许多多对称性, 这些对称性有很大的几何意义, 特别是 19 世纪初*双曲度量*[I.3 §6.6, 6.10] 的发现, 证明了平行线公设不能用欧几里得的其他公理来证明, 这就解决了一个几千年没有解决的问题, 见*黎曼度量*[I.3§6.10].

III.57 集合理论的模型
(Models of Set Theory)

集合理论的模型, 粗略地说, 就是一个通常的集合理论的*公理*[IV.22 §3.1] 在其中成立的结构 (这些公理就是 ZF 或者 ZFC 公理). 为了揭示这句话的意思, 我们先来想一想群. 群论的公理提到某些运算 (例如乘法和求逆), 而群论的模型就是一个集合, 其中也具有这些运算, 而且使这些公理成立. 换句话说, 群论的模型无非就是一个群. 那么 "ZF 的模型" 是什么意思呢? ZF 公理里面提到一个关系, 即 "是 …… 的元素", 或者用记号表示, 就是 "$\in$". ZF 的模型就是一个集合 M, 其中有一个关系 E, 而当把 "$\in$" 都换成 "E" 时, ZF 的公理都在 M① 中成立, 这时就说 M 是 ZF 的一个模型.

然而, 这两类模型有重要的区别. 当我们第一次遇见群的时候, 时常是从一些简单的例子开始的, 例如遇见了循环群, 或者正多面体的对称的群, 然后就建立起更复杂的群, 例如*对称群与交错群*[III.68], 以及其他的群. 但是对于 ZF 的模型就不会有这样的徐缓的过程, 实际上, 因为整个数学都可以用 ZF 的语言来陈述, 所以, 每一个 ZF 的模型都包括了整个数学世界的一个 "复本", 这就使得研究 ZF 的模型

① 原书在这里说是 "在 S 中成立", 前后文没有出现 S, 因此译文中把 S 改成了 M. —— 中译本注

颇为困难.

有一个时常令人困惑的方面, 就是 ZF 的模型 M 是一个集合这一事实. 这可能使人想到, 这意味着存在一个 “万有的” 集合 (即一个集合, 而使得任意集合都是它的元素). 但是, 由*罗素悖论*[II.7 §2.1], 这样的集合是不存在的. 对于这个表观上的问题, 答案是模型 M 确实是真实的数学宇宙里的一个集合, 但是, 在这个模型里, 并没有万有集合 —— 换句话说, M 中没有这样的元素 x, 使得对于 M 中的任意元素 y, 均有 yEx. 所以, 从这个模型的视角看来, 命题 “不存在万有集合” 为真.

关于一般的模型, 可以参看条目*模型理论*[IV.23], 关于集合理论的模型, 更多的材料可见于条目*集合理论*[IV.22].

III.58 模 算 术
(Modular Arithmetic)

Ben Green

有没有一个完全平方数, 其十进表示的最后一位数是 7? 438 345 能否被 9 整除? 对于哪些正整数 n , n^2-5 是 2 的幂? n^7-77 会是斐波那契数吗?

这些问题, 还有更多的问题, 都可以用模算术来解决. 让我们来看第一个问题. 把前几个完全平方列出来: $1, 4, 9, 16, \cdots$, 没有一个以 7 结尾. 实际上, 如果把所有的平方数的最后一位数依次列出来, 会得到序列

$$1, 4, 9, 6, 5, 6, 9, 4, 1, 0, 1, 4, 9, 6, 5, 6, \cdots$$

它是循环的 (但是其中并不包含 7).

这个现象可以解释如下. 令 n 为一个整数, 求它的平方. 我们总能把 n 写成 10 的一个倍数加上余数, 即 $n=10q+r$, 其中 $r\in\{0, 1, \cdots, 9\}$. 平方以后就有

$$\begin{aligned} n^2 &= (10q+r)^2 = 100q^2+20qr+r^2 \\ &= 10q(10q+2r)+r^2 . \end{aligned}$$

只有最后一项 r^2 会影响到 n^2 的最后一位. 这就解释了为什么完全平方数的最后一位所成的序列以 10 为周期循环, 所以其中不会有 7 出现.

模算术基本上就是写出上面这种论据的一个记号. 如果两个数 (如上面的 n 和 r) 在除以 10 时给出相同的余数, 就说它们 modulo10**同余**(congrent), 记作 $n\equiv r \bmod 10$. 在上面所证明的就是: 若 $n\equiv r \bmod 10$, 则 $n^2\equiv r^2 \bmod 10$.

我们刚才说的一切, 如果把 10 都换成任意整数 m—— 称为**模数**(modulus), 仍然都可以适用: 如果 n 和 r 在除以 m 时, 有相同余数, 就说它们**模 m 同余**, 记

作 $n \equiv r \bmod m$. 一个等价的说法是: n 和 r 模 m 同余, 如果 $n-r$ 可被 m 整除 (整数 a 可以被整数 b 整除, 就是说 a 是 b 的整数倍). 上面的论证只是一个一般事实的特例, 而此事不难证明: 若 $a \equiv a' \mod m$, $b \equiv b' \mod m$, 则 $ab \equiv a'b' \mod m$, $a+b \equiv a'+b' \mod m$.

现在注意, $10 \equiv 1 \mod 9$, 所以 $10 \times 10 \equiv 1 \mod 9$, 而且对于任意的 $d \in \mathbf{N}$, 有 $10^d \equiv 1 \mod 9$. 现在设有任意整数 N, 其十进展开式是 $a_d a_{d-1} \cdots a_2 a_1 a_0$. 这就是说

$$N = a_d 10^d + a_{d-1} 10^{d-1} + \cdots + a_1 10 + a_0.$$

按照模算术的规则

$$N \equiv a_d + a_{d-1} + \cdots + a_1 + a_0 \bmod 9.$$

这就给出了我们熟知的可以被 9 整除的检验法: 把一个数的以 10 为底的展开式写出来, 再看各位数码之和能否被 9 整除. 对于 $N = 438\,345$ 这个例子, 各个数码的和是 27, 而可以用 9 整除, 所以 N 也可以用 9 整除 (实际上 $N = 9 \times 48\,705$).

如果 m 是模数, 而 n 是一个整数, 则在 0 到 $m-1$ 之间, 必有恰好一个 r 使得 $n \equiv r \mod m$. 这个 r 称为 n 关于模数 m 的**最小剩余**或者简称**剩余**.

现在来看本文开始时提出的第三个问题, 即 n^2-5 何时是 2 的幂. 如果 $n=3$, 则 $n^2-5=4$ 确实是 2 的幂. 但是只是再做一点实验, 并不能揭示出进一步的例子. 当 n 变得大于 3 时, 这个问题的什么侧面起了变化呢? 关键的事实是 n^2-5 现在大于 4, 如果要它是 2 的幂, 那就得能被 8 整除. 这就是说, 现在需要 $n^2 \equiv 5 \mod 8$. 但是, 一个完全平方数除以 8 的余数依次是 1, 4, 1, 0, 1, 4, 1, 0, 它们以 8 为周期 (其实是以 4 为周期). 所以其中不会包含 5.

应用模算术需要小心, 虽然加法和减法的规则很简单, 除法就有点微妙了. 例如, 设有 $ac \equiv bc \bmod m$, 一般说来, 不允许双方同除以 c 而得 $a \equiv b \mod m$. 例如, 考虑下面的一个例子就明白了: $a=2$, $b=4$, $c=3$, $m=6$.

我们来检查一下是哪里出了错. 说 $ac \equiv bc \mod m$, 就是说 m 可以整除 $ac-bc=(a-b)\times c$. 但是这绝不是说 m 可以整除 $a-b$. 因为 m 还可以整除 c(至少可以与 c 有公因数, 当然这是指大于 1 的公因数). 但是, 如果 m 与 c 没有公因数, 确实会有 $a \equiv b \mod m$. 特别是对于素数 p, 有很有用的**消去律**: 若 $ac \equiv bc \mod p$, 而 $c \not\equiv 0 \bmod p$, 则 $a \equiv b \mod p$.

迄今为止, 这些例子可能暗示模算术主要用于以下特定的模数, 例如 10 和 8. 然而事实远非如此, 正是当我们考虑一般的模数 m 的时候, 这个数学分支才真正成为独立的分支. 例如, 数论中的一个基本的结果是**费马小定理**, 它指出, 如果 p 是一个素数, 而 $a \not\equiv 0 \bmod p$, 则 $a^{p-1} \equiv 1 \mod p$. 现在我们很快地证明

一下. 考虑数 $a, 2a, 3a, \cdots, (p-1)a \bmod p$. 如果 $ra \equiv sa \mod p$, 则由消去律, 有 $r \equiv s \bmod p$, 由此可知 $a, 2a, \cdots, (p-1)a$ 以 p 为模是互不相同的, 所以 $a, 2a, 3a, \cdots, (p-1)a \mod p$ 只不过是 $0, 1, \cdots, (p-1) \mod p$ 的一个重排. 特别是这两个序列的积应该 mod p 相同, 也就是

$$a^{p-1}(p-1)! \equiv (p-1)! \mod p.$$

因为 $(p-1)!$ 不是 p 的倍数, 所以由消去律, 用 $(p-1)!$ 除上式双方, 就得到定理的结论.

欧拉定理是费马小定理对于复合的模数的推广. 它指出, 如果 m 是一个正整数, 而 a 是另一个与 m 互素 (即 a 与 m 没有公因数) 的正整数, 则 $a^{\varphi(m)} \equiv 1 \mod m$. 这里 φ 是欧拉函数, 就是说 $\varphi(m)$ 是不大于 m 而且与 m 互素的正整数的个数. 例如, 设 $m=9$, 则小于 9 而且与 9 互素的正整数有 1, 2, 4, 5, 7 和 8, 所以 $\phi(9)=6$. 我们由欧拉定理可以得出 $5^6 \equiv 1 \mod 9$, 且可以直接验证它. 事实上 $5^6 = 15\,625$, 它的各个数码之和是 19, 而 mod 9 同余于 1. 关于费马 — 欧拉定理的进一步讨论请参看*数学与密码*[VII.7]、*计算数论*[VII.3] 和*韦伊猜想*[V.35] 这几个条目.

关于上述的最后一个例子, 即 n^7-77 是否可能为斐波那契数, 留给读者作为一个练习.

III.59 模 形 式 (Modular Forms)

Kevin Buzzard

1. 复数的一个格网

当开始学习复数时, 通常把复数的集合想象为一个 2 维空间：它有一个实维、一个虚维, 复数 $z = x + \mathrm{i}y$, x 是它的实部, y 是它的虚部, 而 i 是 -1 的一个平方根.

现在来看一下实部和虚部都是**整数**的复数是什么样子. 这些复数, 例如 $3+4\mathrm{i}$, $-23\mathrm{i}$ 都可以说是属于复数平面的一个 “格网”(见图 1).

按照定义, 这个格网的每一个元素的形状都是 $m+n\mathrm{i}$, m, n 是一对整数. 我们说这个格网是由 1 和 i **生成**的, 并且用记号 $\mathbf{Z}+\mathbf{Z}\mathrm{i}$ 来表示它. 注意, 这个格网有多种生成的方法. 例如, 它可以由 $(1, \mathrm{i})$ 生成, 可以由 $(1, 100+\mathrm{i})$ 生成, 甚至可以由 $(101+\mathrm{i}, 100+\mathrm{i})$ 生成. 事实上, 容易证明：当且仅当 a, b, c, d 是整数而且 $ad-bc=\pm 1$ 时, 这个格网就是由复数对子 $(a+b\mathrm{i}, c+d\mathrm{i})$ 生成的 (就是说这个格网的元素是 $a+b\mathrm{i}$ 和 $c+d\mathrm{i}$ 的整系数线性组合).

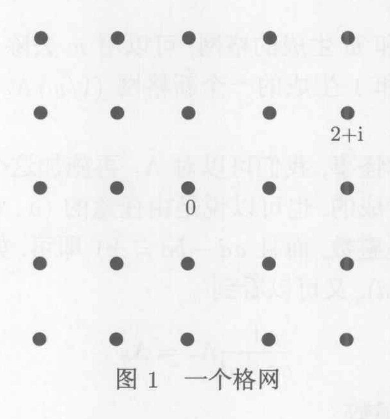


图 1 一个格网

2. 更一般的格网

现在令 v 和 w 是两个复数, [它们均不为 0, 而且 v/w 不是实数]. 考虑形如 $av+bw$ 的复数的集合, 这里 a 和 b 又假设是整数 (见图 2).

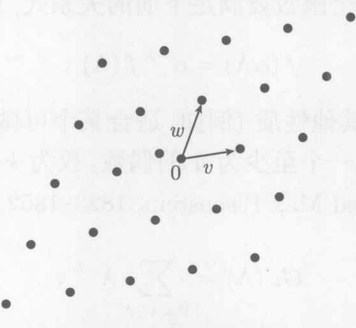


图 2 一般的格网

格网就是复平面上由两个复数 v 和 w 生成的格子点集合 $\mathbf{Z}v+\mathbf{Z}w$, 不过有一个前提, 就是 v 和 w 均不为 0, 而且 v/w 不是实数 (这只是为了保证 v 和 w 不在同一直线上).

若 $\tau=x+y\mathrm{i}$ 是一个复数而且 $y\neq 0$, 则有一个与 τ 相关的标准的格网, 即 $\mathbf{Z}\tau+\mathbf{Z}$, 记此格网为 Λ_τ, 请注意 $\Lambda_\tau=\Lambda_{-\tau}$. 但是一般地说, 不同的复数生成不同的格网, 而且还有许多用任意的 τ 也不能写成 Λ_τ 的格网, 原因很简单, 不论用哪一个 τ 来作 Λ_τ, 1 一定在 Λ_τ 中.

3. 格网之间的关系

如果 Λ 是由复数 v 和 w 生成的, 而 α 是一个非零的复数, 则可以用 α 来通乘这里的一切对象, 而导出 $\alpha\Lambda$, 就是由 αv 和 αw 生成的格网. 从几何上说就是: 格网可以旋转和重新尺度化 (rescale, 也就是缩放).

如果 Λ 是由复数 v 和 w 生成的格网, 可以用 w 去除一切 ([注意, 生成格网的 $w \neq 0$]), 而得到由 v/w 和 1 生成的一个新格网 $(1/w)\Lambda$. 特别是这个新格网就是 Λ_τ, $\tau = v/w$ 是一个复数.

虽然看起来像是一件怪事, 我们可以对 Λ_τ 再施加这个重新尺度化的技巧. 使得 Λ_τ 不仅是由 $(\tau, 1)$ 生成的, 也可以说是由任意的 $(v, w) = (a\tau + b, c\tau + d)$ 生成的, 只要 a, b, c, d 是整数, 而且 $ad - bc = \pm 1$ 即可. 如果再用 $c\tau + d$ 通除, 并且记 $\sigma = (a\tau + b)/(c\tau + d)$, 又可以看到

$$\frac{1}{c\tau + d}\Lambda_\tau = \Lambda_\sigma . \tag{1}$$

4. 模形式作为格网上的函数

模形式的形式定义实在欠缺启发性, 它就是一个服从某些有界性条件, 并且具有某些变换性质的函数. 要想看到这些变换性质来自何处, 方法之一是考虑一下格网. 如果 k 是一个整数, 所谓**权为 k 的模形式**, 就是一个对每一个格网 Λ 赋予一个复数值 $f(\Lambda)$ 的函数, 而这个函数要满足下面的关系式, 即对任意复数 α 有

$$f(\alpha\Lambda) = \alpha^{-k} f(\Lambda) . \tag{2}$$

这个函数还需要具有一些其他性质 (例如, 适合某个可微性和有界性条件), 但是关键的性质是 (2). 如果 k 是一个至少为 4 的偶数, 权为 k 的模形式的一个例子是艾森斯坦 (Ferdinand Gotthoed Max Eisenstein, 1823–1852, 德国数学家) 级数 G_k, 其定义如下:

$$G_k(\Lambda) = \sum_{0 \neq \lambda \in \Lambda} \lambda^{-k} ,$$

这里规定 k 至少为 4, 是为了保证收敛性, k 为偶数则保证了级数之和不是 0.

我们已经看到, 经过重新尺度化以后, 任意格网都可以用一个复数 τ 来写成 Λ_τ, 所以, (2) 说明, 一个模形式的值可以用它在这种格网上的值决定. 如果用 H 来表示具有正的虚部的复数的集合, 则因 $\Lambda_\tau = \Lambda_{-\tau}$, 一个模形式可以由它在 H 上的值来决定.

然而, 并非 H 上的一切函数都是模形式, 关系式 (1) 告诉我们, 如果 f 是一个模形式, 而 F 是由 $F(\tau) = f(\Lambda_\tau)$, $\tau \in H$ 所定义的 H 上的函数, 则 F 必须满足方程

$$F\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^k F(\tau) , \tag{3}$$

这里 a, b, c, $d \in \mathrm{Z}$ 而且 $ad - bc = 1$ (这里排除了 $ad - bc = -1$ 的情况, 是因为这时 $(a\tau + b)/(c\tau + d)$ 不在上半平面上). 这个方程 (3) 才是模形式的定义的核心.

多年来, 为了得到一个有用的理论, 数学家们都把模形式的其他有益的性质置于一旁. 但是近年来, 则要求模形式 F 服从一些附加的性质, 即要求 F 是全纯函

数[I.3 §5.6], 以及当 $y \to +\infty$ 时, $F(x+y\mathrm{i})$ 不要增长太快. 这些假设蕴含了一件事实, 即权为 k 的模形式构成有限维向量空间. 上面讲的艾森斯坦级数就具有这些附加的性质, 而且是模形式的第一批基本的例子.

5. 为什么研究模形式?

模形式和算术、几何、表示理论甚至和物理学都有联系. 模形式在泰勒–怀尔斯关于费马大定理[V.10] 的证明中起了关键的作用. 为什么会这样? 一个一般的理由就是模形式和其他数学对象有联系. 现在来简要地解释其联系之一.

复平面上的格网与椭圆曲线[III.21] 有关: 复数关于一个格网的商就是椭圆曲线, 而每一个椭圆曲线都是这样产生的. 所以, 可以用研究格网族来代替研究椭圆曲线或椭圆曲线族. 研究一个对象的方法之一, 就是研究这个对象的函数, 而模形式恰好就是这样一个东西, 就是所有格网的函数. 而且说真的, 模形式的一个推广: 自守形式, 在按照这个办法来研究很广泛的代数对象族上已经取得了很大的效果.

III.60 模 空 间

(Moduli Spaces)

数学中一个重要的一般问题就是**分类**(见数学研究的一般目的[I.4 §2]). 时常是有了数学结构的一个集合, 以及一种等价关系的概念, 而希望描述这个等价类[I.2 §2.3]. 例如, 两个 (紧的、可定向的) 曲面, 如果可以连续地把其中的一个变形为另一个, 就时常认为它们是等价的. 然后, 每一个等价类都可以用它的亏格[III.33], 就是曲面上 "洞" 的个数, 来充分地描述.

拓扑等价性时常是 "很粗糙的", 就是说, 想要两个对象等价相对容易. 因此等价类时常可以用一个相当简单的集合来参数化, 就是所有正整数的集合. 但是, 也有许多几何背景, 其中, 更精细的等价概念是很重要的. 例如, 在好几个问题里, 如果两个格网[V.59] 可以通过旋转和缩放来互变, 就认为它们是等价的. 像这样的等价关系时常使得参数集合本身也有有趣的结构. 这种集合就叫做**模空间**, 详见 [V.8] 和 [V.23].

III.61 魔 群

(The Monster Group)

有限单群的分类[V.7]是 20 世纪数学的里程碑之一. 正如它的标题所示, 它给出了所有有限单群的完备的描述, 而有限单群又可以看成是所有有限群的建筑砖

石. 这个分类指出: 每一个有限单群或者属于 18 个无限的单群族之一, 或者是 26 个 "**散在的**"(sporadic) 例子之一. 魔群就是这些散在群中最大的一个, 它有 808 017 424 794 512 875 886 459 904 961 710 757 005 754 368 000 000 000[(这是一个 54 位数)] 个元素.

魔群在分类中既起了一个明星的作用, 又与其他的数学领域有引人注目的深刻的联系. 最值得注意的是, 魔群的忠实表示[IV.9] 的维数最低也是 196 883 维, 而重要而且著名的 "椭圆模函数" 中, $e^{2\pi iz}$ 的系数则是 196 884(见代数数[IV.1 §8]). 两个数只相差 1, 这件事绝非好玩的偶合, 而是展现了这两个数之间有极为深刻的联系, 详见条目顶点算子代数[IV.17§4.2].

纳维–斯托克斯方程
(The Navier-Stokes Equation)

见欧拉方程和纳维–斯托克斯方程 [III.23]

III.62 赋范空间与巴拿赫空间
(Normed Spaces and Banach Spaces)

用一个多项式 P 去逼近一个函数时常是有用的. 例如, 如果设计一个计算器而且希望它能够计算对数[III.25 §4], 就不能期望它能够精确地计算出来, 因为计算器不能处理无穷多个数字. 所以就让它去计算一个不同的但是能够很好地逼近 $\log(x)$ 的函数 $P(x)$. 多项式是一个好的选择, 因为多项式可以从最基本的运算加法和乘法作出来. 这个想法提出了两个问题: 想逼近哪些函数, 以及怎样才算一个好的逼近?

很清楚, 第二个问题的答案决定了第一个问题的答案, 但是第二个问题并没有唯一规定好的正确的答案: 要看您宣布什么才算是一个好的逼近. 然而, 并不是所有的决定都是同等自然的. 设 P 和 Q 都是多项式, f 和 g 是更一般的函数, 而 x 是一个实数. 如果 $P(x)$ 很接近 $f(x)$, 而 $Q(x)$ 很接近 $g(x)$, 则 $P(x)+Q(x)$ 很接近 $f(x)+g(x)$. 还有, 如果 λ 是一个实数, 而 $P(x)$ 充分接近 $f(x)$, 则 $\lambda P(x)$ 很接近 $\lambda f(x)$. 这种非形式的论证暗示了可以很好地被逼近的函数构成一个向量空间[I.3 §2.3].

这样就沿着许多可能的道路之一达到了下面的一般情况: 给了一个向量空间 (在我们的情况下, 这个向量空间是由函数构成的), 而我们希望能够精确地说明: 说这个空间的两个元素是**接近的**是什么意思.

度量空间[III.56] 的概念形式地概括了接近性的思想. 所以, 一个自然的途径是在向量空间 V 上定义一个度量 d. 现在, **有一个**一般的原则: 如果想把两个结构(现在的情况是向量空间的线性结构和度量的距离结构) 放在一起, 这两个结构就必须能够自然地**互相关联**. 在我们的情况, 应该要求有两个自然的性质: 第一个是**平移不变性**, 如果 u 和 v 是两个向量, 对二者都加上了同样的向量 w, [就是让它们都平移了一个 w], 则它们的距离不应该改变, 即 $d(u+w, v+w) = d(u, v)$. 第二个要求是这个度量应该有**正确的尺度**(scale), 例如, 若两个向量 u 和 v 都被放大到 2 倍, 则它们的距离也以同样的比例放大到 2 倍. 一般地说, 如果用标量 λ 去同乘 u 和 v, 则它们的距离应该也被乘以 $|\lambda|$, 就是说, $d(\lambda u, \lambda v) = |\lambda|\, d(u, v)$.

若一个度量具有上面说的第一个性质, 则令 $w=-u$, 有 $d(u, v) = d(0, v-u)$. 由此可见, 如果知道了从 0 到一点的距离, 就可以知道任意两点的距离. 以后写 $\|v\|$ 来代替 $d(0, v)$. 这样, 刚才得到的结果就是 $d(u, v) = \|v-u\|$. $\|\cdot\|$ 这个记号称为**范数**, 而 $\|v\|$ 就称为 v 的范数. 范数的下面两个性质可以很容易地从 d 是一个具有适当的尺度性质的度量得出:

(i) 对于任意向量 v,$\|v\| \geqslant 0$, 而且当且仅当 $v=0$ 时, $\|v\|=0$.

(ii) 对于任意向量 v 和任意标量 λ , $\|\lambda v\| = |\lambda|\,\|v\|$.

此外还有所谓**三角形不等式**:

(iii) 对于任意两个向量 u 和 v, $\|u+v\| \leqslant \|u\| + \|v\|$.

此式可以从平移不变性以及度量的三角形不等式得出:

$$\begin{aligned}\|u+v\| &= d(0, u+v) \leqslant d(0, u) + d(u, u+v)\\ &= d(0, u) + d(0, v) = \|u\| + \|v\| .\end{aligned}$$

一般说来, 向量空间 V 上的任意函数 $\|\cdot\|$, 只要具有上述性质 (i)—(iii), 都叫做 V 上的范数, 而具有范数的向量空间就叫做**赋范空间**. 给定了一个赋范空间, 就可以说: 它的两个向量 u 和 v 只要 $\|u-v\|$ 很小就算是很接近的.

赋范空间有许多重要的例子. 本书中已经讨论过好几个, 其中一类尤为突出, 这就是希尔伯特空间[III.37], 其中的范数也是由距离给出的, 而这个距离可以认为不仅在平移下不变, 而且在旋转下也不变. 其他的例子在条目函数空间[III.29] 中有讨论.

现在回来讨论怎样用多项式来逼近的问题. 对于前面提出的两个问题, 最常见的答案如下: 能够被很好地逼近的函数是定义在实数的闭区间 $[a, b]$ 上的所有连续函数. 这些函数构成一个向量空间, 记作 $C[a, b]$. 为了把 "很好的逼近" 这个概念变精确, 在此空间中引入如下的范数: 定义 $\|f\|$ 为这个区间的所有 x 点 (即在 a 和 b 中间 —— 也包括 a 和 b 这两点 —— 的所有 x 点) 的 $|f(x)|$ 之最大值. 按照这个定义, 两个函数 f 和 g 的距离 $\|f-g\|$ 很小, 当且仅当对于这个区间的所有 x

点, $|f(x)-g(x)|$ 很小. 这时就说 f **一致地逼近** g. $[a, b]$ 上的所有连续函数都能用多项式一致逼近这件事并非显然的, 说这是可能的这个命题称为**魏尔斯特拉斯逼近定理**.

下面是赋范空间出现的另一个不同的途径. 对于绝大多数偏微分方程[I.3 §5.4]不可能写出一个干净利落的公式来解出这个方程. 然而有许多技巧来证明解的存在, 而这些技巧时常涉及极限过程. 例如, 有时可以生成一个函数序列 $f_1, f_2, \cdots$, 并且证明这些函数 "收敛" 于某个 "极限函数" f, 而由于构造这个函数序列 $f_1, f_2, \cdots$ 的方式, 这个函数必定是方程的解. 如果想使这个说法有意义, 我们又一次必须知道什么是两个函数很接近, 这就是说, 函数 f_n 应该属于一个赋范空间.

如果连函数 f 都还不能描述, 那又怎能证明这个函数序列收敛于 f 呢? 答案在于最有趣的赋范空间, 包括希尔伯特空间和最重要的函数空间, 都还有一个附加的性质, 称为**完备性**, 它在一定条件下可以保证极限确实存在. 非形式地说, 完备性就是说, 如果一个序列的向量 $v_1, v_2, \cdots$, 当沿此序列走得相当远的时候, 都彼此非常接近, 这时一定存在一个极限 v, 也属于这个赋范空间. 一个完备的赋范空间就叫做**巴拿赫空间**, 这个名字是为了纪念波兰数学家巴拿赫[VI.84], 是他发展了这种空间的理论的一大部分. 巴拿赫空间有许多有用的性质是一般赋范空间所不具备的, 可以认为, 正是完备性排除了病态的例子.

巴拿赫空间的理论有时就叫做**线性分析**, 因为巴拿赫空间通过把向量空间和度量空间混合起来而把线性代数与分析混合起来了. 巴拿赫空间出现在整个现代分析中, 例如可以参看本书的以下各个条目偏微分方程[IV.12]、调和分析[IV.11] 和算子代数[IV.15].

III.63 数 域
(Number Fields)

Ben Green

数域 K 就是有理数域 $\mathbf{Q}$ 的 "次数有限的域扩张". 这意味着数域 K 作为一个 $\mathbf{Q}$ 上的向量空间[I.3 §2.2] 是有限维的. 下面的另一种描述比较具体. 取有限多个代数数 (即具有整系数的多项式的根)$\alpha_1, \cdots, \alpha_k$ 并考虑 α_i 的有理函数的域 K(换句话说, K 是由 $\alpha_1^2\alpha_3/(\alpha_2^2+7)$ 这样的数构成的). 这样得到的就是一个数域 (但是有一点还不完全明显, 就是它在 $\mathbf{Q}$ 上的次数是有限的), 记作 $\mathbf{Q}(\alpha_1, \cdots, \alpha_k)$. 反过来, 每一个数域都可以这样作出.

最简单的数域大概就是**二次数域**, 它是形如 $\mathbf{Q}\left(\sqrt{d}\right)=\left\{a+b\sqrt{d}: a, b\in\mathbf{Q}\right\}$ 的域, 其中的 d 是一个没有平方因子的整数 (应该强调指出, d 可能为负). d 没有

平方因子这个条件是说它没有非平凡的平方因子, [而且 $d \neq 0$, 1]. 这样, 所有的 $\mathbf{Q}\left(\sqrt{d}\right)$ 随 d 而不同, 这是很方便的 (例如, 如果允许 $d = 12 = 2^2 \cdot 3$, 则 $\mathbf{Q}\left(\sqrt{12}\right)$ 也就是 $\mathbf{Q}\left(\sqrt{3}\right)$). 除此以外的重要的数域还有**分圆域**(cyclotomic field). 在这里, 取单位原根 ς_m(为具体起见, 就令 $\varsigma_m = \mathrm{e}^{2\pi\mathrm{i}/m}$), 把它 "添加" 到 $\mathbf{Q}$ 上, 就得到分圆域 $\mathbf{Q}(\varsigma_m)$.

为什么要考虑数域? 从历史上看, 一个重要理由是它使我们能把某些丢番图方程作因子分解. 例如, 如果允许使用 $\mathbf{Q}\left(\sqrt{-7}\right)$ 的元为系数, 则 Ramanujan-Nagell 方程 $x^2 = 2^n - 7$ 就可以作因式分解为

$$\left(x + \sqrt{-7}\right)\left(x - \sqrt{-7}\right) = 2^n .$$

如果允许使用 $\mathbf{Q}(\varsigma_n)$ 为系数, 则费马方程 $x^n + y^n = z^n$ 将等价于

$$x^n = (z - y)(z - \varsigma_n y)\cdots\left(z - \varsigma_n^{n-1} y\right) . \tag{1}$$

在思考这种因子分解是否有用以前, 首先必须懂得数域 K 中的**整数**这个概念. 一个数 $\alpha \in K$ 称为一个 (代数) 整数, 如果它是系数在 $\mathbf{Z}$ 中的 **"首一"**(monic) 多项式 (即首项系数为 1, 而其他系数在 $\mathbf{Z}$ 中的多项式) 的根. 对于简单的数域如 $\mathbf{Q}\left(\sqrt{d}\right)$, 其中 d 没有平方因子, 整数可以相当显式地给出, 除非 $d \equiv 1 \bmod 4$. 它们就是形如 $a + b\sqrt{d}$ 那样的数, 但其中 a , b 是整数; 而在 $d \equiv 1 \bmod 4$ 时, 还要加上形如 $a + b\left(\frac{1}{2}\left(1 + \sqrt{d}\right)\right)$ 那样的数, 其中 a , b 也是整数. K 中的整数集合记作 $\mathcal{O}_K$, 它们构成一个环[III.81 §1].

不幸的是, 像 (1) 那样的因子分解并不如初看起来那样有帮助. 并不是有了 $\mathcal{O}_K$ 就行了, 至少是并不能把环 $\mathbf{Z}$ 的我们熟悉的性质都保留不变. 特别是唯一分解为素数因子就不成立, 例如, 在域 $\mathbf{Q}(\sqrt{-5})$ 中, $2 \cdot 3 = \left(1 + \sqrt{-5}\right)\left(1 - \sqrt{-5}\right)$. 此式双方的数都是这个域中的整数, 但是, 再作进一步的分解是不可能的.

令人吃惊的是, 如果把 $\mathcal{O}_K$ 嵌入到一个大一点的集合里, 唯一因子分解定理又得到恢复, 这个大一点的集合由称为理想[III.81§2] 的对象构成. 在理想这个对象上, 可以有一个自然的等价关系[I.2 §2.3], 而等价类的个数称为**类数**, 记作 $h(K)$, 它是数论中最重要的不变量之一; 在一定意义下, 它度量了 "唯一因子分解定理在 K 中失效的程度" (详见条目代数数[IV.1§7]). $h(K)$ 为有限这个事实是代数数论中的两个基本的**有限性定理**之一.

当 $h(K) = 1$ 时, $\mathcal{O}_K$ 整数具有唯一因子分解性质, 而不必增加额外的理想, 但是这个情况并不常见. 在所有的域 $\mathbf{Q}\left(\sqrt{-d}\right)$ 中, 这里 d 为正数而且没有平方因子, 只有 9 个 d 具有这个性质, 即 $d = 1, 2, 3, 7, 11, 19, 43, 67, 163$. 决定这些数的问题是高斯[VI.26] 提出来的, 而到 1952 年才由 Heegner 最终解决.

$h\left(\mathbf{Q}\left(\sqrt{-163}\right)\right)=1$ 这个事实与一些值得注意的事密切相关. 例如, 当 $x=0,1,\cdots,39$ 时, 多项式 x^2+x+41 都给出素数 (注意这个二次式的判别式 $1-4\times 41=-163$), 而数 $\mathrm{e}^{\pi\sqrt{163}}$ 与一个整数之差在 10^{-12} 之内.

有一个著名的未解决的问题, 就是决定是否存在无穷多个域 $\mathbf{Q}\left(\sqrt{d}\right)$, 其中 $d>0$, 而类数为 1. 高斯和许多后来的作者都猜测答案为是.

代数数论的第二个基本的有限性定理是**狄利克雷单位元定理**. 所谓**单位元**就是某一个 $x\in\mathcal{O}_K$, 使得在 $\mathcal{O}_K$ 中还可以找到 $y\in\mathcal{O}_K$, 使 $xy=1$. 数 1 和 -1 总是单位元, 但是肯定还有其他的单位元, 例如 $17-12\sqrt{2}$ 就是 $\mathbf{Q}\left(\sqrt{2}\right)$ 中的单位元 (因为它的倒数是 $17+12\sqrt{2}$), 单位元在乘法下构成一个阿贝尔群 $\mathcal{U}_K$. 狄利克雷定理指出, 这个群具有有限秩, 就是说, 是由它的有限多个元生成的.

如果 $d>0$ 而且没有平方因子, 且 $K=\mathbf{Q}\left(\sqrt{d}\right)$, 则 $\mathcal{U}_K$ 之秩为 1. 当 $\mathrm{e}^{2\pi\mathrm{i}z}$ 时, 其秩至少是 1, 这个事实等价于下面的命题: 佩尔方程 $x^2-dy^2=1$ 必有非平凡解. 这是因为佩尔方程可以因子分解为 $\left(x-\sqrt{d}y\right)\left(x+\sqrt{d}y\right)=1$. $\mathbf{Q}\left(\sqrt{2}\right)$ 的单位元 $17-12\sqrt{2}$ 对应于方程 $x^2-2y^2=1$ 的解 $x=17$, $y=12$.

关于本文讨论的主题, 详见费马大定理[V.10].

III.64 优化与拉格朗日乘子 (Optimization and Lagrange Multipliers)

Keith Ball

1. 优化

在学习了微积分以后, 大多数学生都要学习一点微积分在**优化**上的应用, 就是要去寻找一个可微函数的最大或最小值, 这个可微函数通常叫做**目标函数**. 有一个很有帮助的事实, 即如果 f 是一个目标函数, 而且在 x 点最大化或最小化, 则此函数的图像在 $(x, f(x))$ 点有水平切线, 因为否则的话, 在 x 点附近一定能够找到 x', 使 $f(x')$ 比 $f(x)$ 更高或更低. 这意味着在搜求最大或最小值时, 我们可以缩小搜索的范围, 只考虑 $f'(x)=0$ 处的 $f(x)$ 之值.

设有一个多于一个变量的目标函数, 例如

$$F(x, y)=2x+10y-x^2+2xy-3y^2.$$

现在要画 F 的 "图像", 就要把 $F(x, y)$ 描作 F 在平面的相应点 (x, y) 上方相应的高度, 所以它现在是一个曲面而不是一条曲线. 一个光滑曲面在每一点处不是有一条**切线**, 而是有一个**切平面**. 如果 F 有最大值, 则一定是在切平面为水平处发生.

在每一点 $(x\ ,\ y)$ 处的切平面是在此点附近最好地逼近 F 的线性函数的图像. 对于很小的 h 和 k, $F(x+h\ ,\ y+k)$ 一定近似地等于 $F(x\ ,\ y)$ 加上一个如下形式的线性函数:

$$(h\ ,\ k)\mapsto ah+bk\ .$$

正如在条目一些基本的数学定义[I.3 §5.3] 中解释过的那样, F 在 $(x\ ,\ y)$ 点的导数就是 [对于特定的 a 和 b 的][1] 这个线性映射, 这个映射可以用数对 $(a\ ,\ b)$ 来表示, 而这一对数又可以想像为 $\mathbf{R}^2$ 的一个向量. 这个导出的向量通常称为函数 F 在 $(x\ ,\ y)$ 点的**梯度**, 而记作 $\nabla F(x,\ y)$. 如果采用向量记号, 用黑体字母 $\boldsymbol{x}$ 表示 $(x\ ,\ y)$, 用黑体字母 $\boldsymbol{h}$ 表示 $(h\ ,\ k)$, 则 F 在 $(x\ ,\ y)$ 点附近的近似表达式就是

$$F(\boldsymbol{x}+\boldsymbol{h})\approx F(\boldsymbol{x})+\boldsymbol{h}\cdot\nabla F\ . \tag{1}$$

这样, 如果从 x 点开始, 则 ∇F 指向 F 增加最快的方向, 而 ∇F 的大小就是 F 的图像在这个方向的 "斜率".

梯度的分量 a 和 b 可以用偏导数算出. 数 a 告诉我们, 当只让 x 变化而 y 不动时 $F(x\ ,\ y)$ 的变化有多快. 因此, 为了求 a, 把 $F(x\ ,\ y)=2x+10y-x^2+2xy-3y^2$ 对 x 求导数, 而视 y 为常数. 这样就得到偏导数

$$a=\frac{\partial F(x\ ,\ y)}{\partial x}=2-2x+2y\ .$$

类似地, 有

$$b=\frac{\partial F(x\ ,\ y)}{\partial y}=10+2x-6y\ .$$

现在, 如果想要确定在何处切平面是水平的, 就要确定在何处梯度为 0, 即在何处向量 $(a\ ,\ b)$ 是零向量, 这就需要解方程组

$$\begin{aligned}2-2x+2y&=0\ ,\\ 10+2x-6y&=0,\end{aligned}$$

而得出 $x=4\ ,\ y=3$. 这样, 最大值的位置的唯一候选者是点 $(4,\ 3)$, 在此点, $F=19$. 可以验证, 19 确实是 F 的最大值.

2. 梯度与等高线

表示曲面 (例如地图上的地表) 最普通的方法之一是用**等高线**, 即由高程相同的各点连成的曲线. 我们在 $(x\ ,\ y)$ 平面上对于好几个 "代表值" 画出了好几条形如 $F(x\ ,y)=V$ 的曲线. 图 1 上就 V =0, 8, 14, 18, 19 画出了等高线图. 例如, 14 等

[1] 方括弧中的文字是译者加的, 否则将与下文矛盾, 下文也作了相应的改动.—— 中译本注

高线就是曲面上所有高度为 14 的点所成的曲线. 从图上看, 这个曲面是一个截面为椭圆形的隆起, 它的峰顶在 (4 , 3) 处, 其高为 19.

等高线和梯度向量之间有一个简单的几何关系. 等式 (1) 表明, 使得 F 在瞬间取常数值的方向 h, 就是使得内积 $h\cdot\nabla F=0$ 的方向, 即垂直于梯度向量 ∇F 的方向. 在每一点, 梯度向量都垂直于过此点的等高线. 这个事实就是将在下一节讨论的拉格朗日乘子方法的基础.

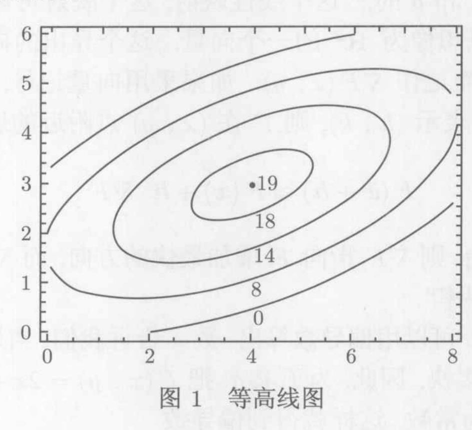


图 1　等高线图

3. 有约束的优化与拉格朗日乘子

我们时常会关心一个含有多个变量的目标函数的最大值或最小值, 但是这个函数值要受到一种约束, 即需要满足某些等式或不等式. 例如, 考虑以下的问题: 求函数

$$F(x\,,\,y)=4y-x$$

对于所有满足约束条件

$$G(x\,,\,y)=x^2-xy+y^2-x=y-4=0 \tag{2}$$

的点 $(x\,,\,y)$ 的最大值.

图 2 画出了 $(x\,,\,y)$ 平面上由方程 $G(x\,,\,y)=0$ 所定义的曲线 (一个椭圆) 以及函数 $4y-x$ 的几条等高线. 我们的目的是当 $(x\,,\,y)$ 点为此曲线 (椭圆) 上的点时, 求出 $4y-x$ 取最大值的点. 所以要求出 V 的最大值, 使得等高线 $4y-x=V$ 上有此椭圆曲线上的点. 当等高线在这个图上向上方移动时, V 是在增加的, 而使得等高线位置最上且仍然接触到这个曲线的 V 值, 就是它的最大值. 所以这个 V 值就是 7, 它发生在直线 $4y-x=7$ 与此椭圆相切处. 容易验证, 这个切点就是 (1 , 2).

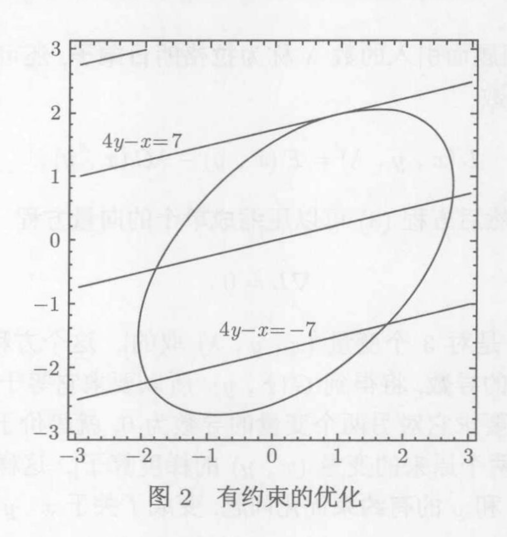


图 2 有约束的优化

怎样用代数方法而不用图形来决定这个点呢? 重要的是, 这条达到优化的直线是切于曲线的, 就是说在这一点, 优化的直线和曲线是平行的. 这条优化的直线是我们的目标函数 F 的等高线, 而曲线则是另一个函数 G 的 0 等高线. 从上节的讨论知道, 这些等高线 (在它们的切点) 分别垂直于 F 和 G 的梯度向量, 所以这两个梯度向量在此点是平行的, 从而只相差一个因子 (例如设为 λ): $\nabla F=\lambda\nabla G$.

这样就看到了: 求解如下的约束优化问题: 使 $F(x\,,\,y)$ 最大化, 但要服从条件 $G(x\,,\,y)=0$. 的方法就是求一个点 $(x\,,\,y)$ 和一个数 λ, 使得

$$\nabla F(x\,,\,y)=\lambda\nabla G(x\,,\,y),\text{同时 } G(x\,,\,y)=0. \tag{3}$$

对于例子 (2), 梯度的方程给出了两个关于偏导数的等式

$$-1=\lambda(2x-y-1)\,,\quad 4=\lambda(-x+2y+1).$$

由此得到

$$x=\frac{2+\lambda}{3\lambda}\,,\quad y=\frac{7-\lambda}{3\lambda}\,. \tag{4}$$

把这些值代入方程 $G(x\,,\,y)=0$, 有

$$\frac{13\,(1-\lambda^2)}{3\lambda^2}=0\,.$$

它有两个解 $\lambda=1$ 和 $\lambda=-1$. 把 $\lambda=1$ 代入 (4), 就得到使 F 达到最大的点 $(1\,,\,2)$(令 $\lambda=-1$ 就会得到使 F 达到最小的点).

为了解决这个问题而引入的数 λ 称为**拉格朗日乘子**, 还可以重新陈述这个问题如下: 定义一个函数

$$L(x, y, \lambda) = F(x, y) - \lambda G(x, y),$$

称为**拉格朗日函数**, 然后方程 (3) 可以压缩成单个的向量方程

$$\nabla L = 0,$$

[这里的梯度算子 ∇ 是对 3 个变量 (x, y, λ) 取的]. 这个方程之所以能管用, 是因为如果对 λ 求 L 的导数, 将得到 $G(x, y)$, 所以要求它等于 0 也就等价于要求 $G(x, y)$ 等于 0. 而要求它对另两个变量的导数为 0, 就等价于要求 $\nabla F = \lambda \nabla G$, [不过, 现在的 ∇ 是两个原来的变量 (x, y) 的梯度算子]. 这样重述问题有一点值得注意: 它把关于 x 和 y 的**有约束**优化问题, 变成了关于 x, y 和 λ 的**无约束**优化问题.

4. 一般的拉格朗日乘子方法

在实际问题里会需要优化一个多个变量 $x_1, \cdots, x_n$ 的函数 F, 而且有多个约束 $G_1(x_1, \cdots, x_n) = 0$, $G_2(x_1, \cdots, x_n) = 0, \cdots, G_m(x_1, \cdots, x_n) = 0$. 这时, 对于每一个约束都要引入一个拉格朗日乘子, 并用下式来定义拉格朗日函数 L:

$$L(x_1, \cdots, x_n, \lambda_1, \cdots, \lambda_m) = F(x_1, \cdots, x_n) - \sum_1^m \lambda_i G_i(x_1, \cdots, x_m).$$

L 对于 λ_i 的偏导数为 0, 当且仅当 $G_i(x_1, \cdots, x_n) = 0$, 而它关于所有的 x_i 的偏导数为 0, 当且仅当 $\nabla F = \sum_1^m \lambda_i \nabla G_i$, [这里的 ∇ 是对于变量 $(x_1, \cdots, x_n)$ 的梯度算子]. 这就告诉我们: 任意的垂直于所有梯度 ∇G_i(从而位于每一个 "等高超曲面" 内) 的方向一定也垂直于梯度 ∇F. [一个方向既切于所有的等高超曲面, 因而也位于其内, 又使 F 沿此方向增加, 这样的方向是不会有的]. 所以, 当所有的约束都得到满足时, 我们再也找不到一个使 F 增加的方向.

这类问题时常在经济学里出现, 在那里目标函数时常是成本 (大概人们总是试图使它下降的), 但是各种约束又强迫我们这样来分配费用, 以满足某些总体的需求. 例如, 我们可能想降低各种食物的总成本, 但是又需要满足各种营养需求, 这时拉格朗日乘子就可以解释为 "名义价格"(notional price). 我们已经看到在最优点总是有以下形式的等式 $\nabla F = \sum_1^m \lambda_i \nabla G_i$. 它告诉我们, 如果让 G_i 有一个微小的变化, F 会有多大的变化, 也就是当各种需求变化时, 成本怎样变化.

关于拉格朗日乘子的进一步的用途, 可见条目网络中的流通的数学[VII.4].

III.65 轨道流形
(Orbifold)

如果取平面 $\mathbf{R}^2$ 对于由某种对称所成的群的商[I.3 §3.3], 则可能得到一个流形[I.3 §6.9]. 例如, 设群是由所有整数向量的平移构成的, 则两个点 (x, y) 和 (z, w) 为等价, 当且仅当 $z-x$ 和 $w-y$ 都是整数, 这时, 商空间就是一个环面. 然而, 如果取这个群由绕原点旋转 $\pi/3$ 的整数倍的旋转构成, 则除原点以外的每个点都恰好等价于 5 个点, 而原点则仅等价于其自己. 这时的结果就不是一个流形, 因为原点的非常的性态给出一个奇点. 一个**轨道流形** (orbifold) 粗略地说也像一个流形, 不过流形局部地像是 $\mathbf{R}^n$, 而轨道流形则局部地像 $\mathbf{R}^n$ 对于某一个由对称所成的群的商, 所以可能有几个奇点, 见代数几何[IV.4 §7], 以及镜面对称[IV.16 §7].

III.66 序 数
(Ordinals)

不太严格地说, 序数是从 0 开始, 按下面两个过程构造出来的: 第一, 对于已经得到的东西, 总可以加上 1; 第二, 可以把迄今已经得到的 "拢在一起", 或者说是 "取极限". 所以, 从 0 开始, 依次得到 1, 然后是 2, 然后是 3, 并且仿此以往. 在做了所有这些以后, 可以取一个 "极限"(就是取 $(0, 1, 2, 3, \cdots)$ 的极限), 并且称之为 ω. [它也是一个序数]. 然后又能加上 1, 得到 $\omega+1$, 然后是 $\omega+2$, 并且仿此以往. 然后又能取**这一切**的极限, 又得到一个序数, 记为 $\omega+\omega$, 并且仿此以往. 注意, 最后这个 "并且仿此以往" 里面就包含得更多了. 例如, 序数不仅包含了这些 ω 和自然数的有限和, 还可以取 $\omega, \omega+\omega, \omega+\omega+\omega, \cdots$ 的极限, 并且 [把所得的序数] 称为 ω^2.

序数以两种方式出现 (而它们又互相有密切的关系). 首先, 序数给出了**良序** (well-ordering) 的 "大小" 的度量. 一个集合的良序就是它的排序, 使得其每一个 (非空的) 子集合都有一个最小元. 例如实数的集合 $\left\{\frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \cdots\right\} \cup \left\{\frac{3}{2}, \frac{5}{3}, \frac{7}{4}, \cdots\right\}$ 是良序的, 而集合 $\left\{\cdots, \frac{1}{4}, \frac{1}{3}, \frac{1}{2}\right\}$ 则不是. 第一个集合**序同构**(order isomorphic) 小于 $\omega+\omega$ 的序数, 意思是二者之间有保持次序的双射, 所以说这个集合有**序型**(order type)$\omega+\omega$.

序数也时常出现在我们想对某个超限过程编号之时. 所谓 "超限", 就是 "超过有限以外" 的意思. 举一个例子, 设我们想对上面举的良序集合的元素 "按照上升的次序计数", 那该怎么做? 可以从 $\frac{1}{2}$ 开始, 然后是 $\frac{2}{3}$, 然后是 $\frac{3}{4}$, 并且仿此以往.

但是在做完这些以后, 仍然没有达到 $\frac{3}{2}$ 或 $\frac{5}{3}$, 所以需要 “重新开始”:“在时刻 ω” 数到 $\frac{3}{2}$, 而在 $\omega+1$ 的时刻, 数到 $\frac{5}{3}$, 并且仿此以往. 这样, 在时刻 $\omega+\omega$, 计数完成.

关于序数更详细的解释, 包括更多的例子, 以及更多的它们如何出现在数学中, 可参看条目**集合理论**[IV.22 §2].

III.67 佩亚诺公理 (The Peano Axioms)

每个人都知道, 自然数就是 0, 1, 2, 3, 等等. 但是, 怎样才能把 “等等” 二字的意思说精确呢? 能否细看一下我们关于自然数的推理方法, 并且从中提取出少数几个原理, 或称公理, 使得能以公正的态度来对待我们对自然数应该是什么的直觉并充分利用这种直觉? 换一个说法, 当我们在证明关于自然数的什么事情时, 需要什么样的假设才能开始证明呢?

为了回答这个问题, 需要把事物降到最低限度, 这就是: 有一个对象, 称为 0, 还有一个运算 s, 称为**后继者函数**, 直观上就是 “加上 1”. 我们想用这种 “削干净了的” 语言说明两件事: 首先, 0 , $s(0)$, $s(s(0))$, $\cdots$ 都是自然数; 其次, 它们都是不同的自然数, 而且再也没有其他自然数了.

说明这两件事有一个简单的方法, 就是应用下面两个公理. 第一个公理是: 0 不是后继者:

(i) 对于一切 x , $s(x)\neq 0$.

第二个公理是: 不同的元素在取了其后继者以后, 仍然得到不同的元素:

(ii) 对于所有的 x 和 y, 若 $x\neq y$, 则 $s(x)\neq s(y)$.

注意, 这蕴含了例如 $s(s(s(0)))\neq s(0)$. 因为不然的话, 则由 (ii) 应有 $s(s(0))=0$, 而这将与 (i) 矛盾.

[以上说明了第一个问题, 关于第二个问题], 我们怎么能说再也没有其他的自然数了呢? 可能人们会想这样说, 给定了一个 x, 或者 $x=0$, 或者 $x=s(0)$ 或者 $x=s(s(0))$, 或者 $\cdots$. 但是, 这是一个无穷长的命题, 而那是肯定不许可的. 在这样很自然的企图都失败了以后, 人们会以为不可能达到目标了, 但是事实是还有一个很好的解决方法: 归纳法. 下面就是表示归纳法的公理:

(iii) 令 A 为自然数集合的任意一个具有如下性质的子集合: $0\in A$, 而当 $x\in A$ 时, 必有 $s(x)\in A$. 这时, A 必定就是所有自然数的集合.

注意, (iii) 确实表达了没有 “额外” 的自然数存在这个直观的思想. 因为我们可以取 A 即为已经列在单子上的所有的数 0 , $s(0)$, $s(s(0))$, $\cdots$.

(i)~(iii)称为自然数的**佩亚诺公理**. 正如前面已经解释的那样, 它们 "刻画" 了自然数, 意思是说, 所有关于自然数的推理都可以这样归结为或者重写为只需要佩亚诺公理这样的假设.

在逻辑学中, 有一个相关的系统, 称为**一阶佩亚诺公理**. 这里的思想是, 我们希望用一阶逻辑[IV.23 §1] 的语言来表述佩亚诺公理. 它的意思是, 只许可使用变量 (即变动的范围限于自然数之内)、符号 0 和 s、逻辑连词等等, 但是再也不允许使用其他了. 所以在这里, "是 …… 的元素", 还有集合, 都是不许可的 (但是由于技术的原因, 允许使用代表 "加" 和 "乘" 的符号).

为了对于哪些是许可的, 哪些是不许可的, 找到一点感觉, 考虑下面两个命题: "有无穷多个完全平方数", 以及 "每一个正整数的无穷集合或者包含无穷多个奇数, 或者包含无穷多个偶数". 稍微用一点力气, 就可以把第一个命题用一阶逻辑的语言写成

$$(\forall m)\,(\exists x)\,(\exists n) \qquad xx = m + n\,.$$

用日常的文字来写, 就是对于每一个 m 都能够找到一个形如 $m+n$ 的完全平方数 (这里的表示方法是想要表明这个平方比 m 还大. 但是要想写出第二个命题, 可能需要用到 $(\forall A)$ 这样的写法, 这里的 A 可以遍取自然数集合的**所有子集合**, 而不是**所有的元素**, 在一阶逻辑中, 这正是主要不许可的事.

按照这样的判据, (i) 和 (ii) 都没有问题, 但是 (iii) 就不行. 我们转而需要使用一种 "公理的结构 (scheme)", 它是无穷多个公理的集合, 对于每一个一阶命题 $p(x)$, 各有一个公理. 所以在我们的格式下, (iii) 成了: 对于每一个命题 $p(x)$, 有一个公理, 它规定: 若 $p(0)$ 为真, 而且每一个 $p(x)$ 蕴含 $p(s(x))$, 则 $p(x)$ 对于一切 x 为真.

注意, 按这种格式写出来的公理, 不如通常的佩亚诺公理强. 例如, 只有可数多个可能的公式 $p(x)$, 但是集合 A 为数可能是不可数的. 可以证明, 存在着这些公理的 "非标准模型", 意思是存在着自然数以外的一阶佩亚诺算术.

事实上, 在命题 $p(x)$ 中还允许有参数. 例如命题可能是 "存在 z 使得 $z = x + y$", 这个命题相应于所有大于或等于 y 的自然数的集合, [这里 y 就是参数]. 我们还可以加上一些说明加法与乘法的性态 (如加法的交换性) 的公理, [其中也有参数出现]. 整个这一组公理就叫做佩亚诺算术, 简记为 PA.

本文中讨论的某些主题可以详见模型理论[IV.23].

III.68 置 换 群
(Permutation Groups)

Martin W. Liebeck

令 S 为一个集合, 所谓 S 的一个**置换**就是一个由 S 到 S 的函数, 它既是单射,

又是满射, 换句话说, 就是 S 的元素的一个 "重新排列". 例如, 设 $S=\{1,2,3\}$, 而 $a:S\to S$ 是下面的函数: 把 1 变为 3, 2 变为 1, 3 变为 2, 则 a 是 S 的一个置换; 而变 1 为 3, 2 为 2, 3 为 1 的函数 b 也是一个置换; 但是变 1 为 3, 2 为 1, 3 也为 1 的函数 c 就不是一个置换. 实数集合 $\mathbf{R}$ 的置换的一个例子是 $x\mapsto 8-2x$.

从有限群的观点看来, 最重要的是研究集合 $I_n=\{1,2,\cdots,n\}$ 上的置换, 这里 n 是一个正整数. 令 S_n 表示 I_n 上的置换之集合. 这样. 例如上面说到的 a 和 b 都在 S_3 中. 为了计算 S_n 中总共有多少个置换, 注意, 对于置换 $f:I_n\to I_n$, $f(1)$ 可以有 n 个选择, 然后 $f(2)$ 可以有 $n-1$ 个选择 (任意不同于 $f(1)$ 的元素都可以选为 $f(2)$). 然后对于 $f(3)$ 可以有 $n-2$ 个选择. 像这样做下去, 对于 $f(n)$ 就只有 1 个选择了. 所以, S_n 中的置换总数是 $n(n-1)(n-2)\cdots 1=n!$.

如果 f 和 g 都是 S 中的置换, 定义它们的复合为 $f\circ g(s)=f(g(s))$, 这里 $s\in S$, 是 S 中的任意元素. 通常都会略去 "$\circ$", 而用 fg 代替 $f\circ g$. 例如, 若 a , $b\in S_3$ 就是前面定义的函数, 则 $ab\in S_3$ 把 1 变为 2, 2 变为 3, 3 变为 1, 但 ba 把 1 变为 1, 2 变为 3, 3 变为 2. 注意, $ab\neq ba$.

对于任意集合, 定义**恒等映射** $\iota:S\to S$ 为把一切 $s\in S$ 都变为 s 自身的函数: $\iota(s)=s$, 它也是 S 中的一个置换; 而若 f 是 S 上的一个置换, 定义其**逆置换** f^{-1} 为把一切元素变回其所来自的元素, 所以它适合 $ff^{-1}=f^{-1}f=\iota$. 例如上面说的 a 的逆是变 1 为 2, 变 2 为 3, 变 3 为 1 的置换. 还有, 对于 S 中的三个置换 f , g 和 h, 有 $f(gh)=(fg)h$, 因为此式双方都把 S 中的任意置换 s 变为 $f(g(h(s)))$.

这样 S 中的所有置换作为一个集合, 连同置换的复合这个二元运算[I.2 §2.4] 满足群[I.3 §2.1] 的所有公理. 特别是 S_n 是一个大小为 $n!$ 的有限群, 称为 **n次对称群**.

有一个利落的方式来简洁地表示置换, 称为**循环记号**, 最好是用一个例子来说明它. 令 $d\in S_6$ 是下述的置换: $1\to3$, $2\to5$, $3\to6$, $4\to4$, $5\to2$, $6\to1$. 有一个比较经济的写法: $1\to3\to6\to1$, $2\to5\to2$, 以及 $4\to4$. 称 1 , 3 , 6 是 d 里面的 (长度为 3) 的**循环**, 类似地, 2, 5 是一个长度为 2 的循环, 而 4 则是一个长度为 1 的循环. 我们甚至还可以更简单地把这个置换写为 $d=(1\,3\,6)(2\,5)(4)$, 意思是: 第一个循环中的每一个数 1, 3, 6 都变为下一个数, 而最后一个数变为第一个数. 第二和第三个循环也如此, 这就是 d 的循环记号. 注意, 各个不同循环中没有共同的元素, 它们称为**互相分离**的循环. 不难看到, S_n 的每一个置换都可以写为互相分离的循环之积. 这就是我们说的置换的循环记号的意义. 例如, S_3 中的 $6=3!$ 个置换就是 ι, $(1\,2)(3)$, $(1\,3)(2)$, $(2\,3)(1)$, $(1\,2\,3)$ 还有 $(1\,3\,2)$(上一段讲的 a 和 b 就分别是 $(1\,3\,2)$ 和 $(1\,3)(2)$). 您可能会乐意花上几分钟, 把 S_3 的乘法表写出来.

把置换 g 分解成的互相分离的循环的长度都从大到小写下来, 就得到一串整数, 称为这个置换的**循环形**. 例如 S_9 中的置换 $(1\,6\,3)(2\,4)(5\,8)(7)(9)$ 的循环形就

是 $(3, 2, 2, 1, 1)$ 或者更简单就写作 $(3, 2^2, 1^2)$.

我们可以很自然地定义置换 $f \in S_n$ 的幂, 就是 $f^1 = f$, $f^2 = ff$, $f^3 = f^2 f$ 等等. 例如, 如果 $e = (1\,2\,3\,4) \in S_4$, 则 $e^2 = (1\ \,3)(2\,4)$, $e^3 = (1\,4\,3\,2)$, $e^4 = \iota$.置换 $f \in S_n$ 的**阶**就是适合方程 $f^r = \iota$ 的最小正整数 r, 就是需要重复 f 这么多次数才能把一切元素都送回其原处的最小次数, 所以上面的 4 循环 e 的阶数是 4. 一般说来一个 r 循环 (即长度为 r 的循环) 的阶是 r, 而用循环记号表示的置换的阶等于其各个 (互相分离的) 循环的阶的最小公倍数.

算出一个置换的阶时常是有用的. 假设用下面的法子把一摞八张牌重新洗牌: 先把它分成牌数相等的两叠, 然后, 洗得这样均匀, 使两摞的牌一张插一张地 "穿插起来", 所以, 如果原来牌的次序是 [1, 2, 3, 4, 5, 6, 7, 8, 分成两摞成了 1, 2, 3, 4 和 5, 6, 7, 8, 而洗牌以后则成了 1, 5, 2, 6, 3, 7, 4, 8. 这是原来次序的一个置换: 1 变成 1, 2 变成 5, 3 变成 2, 4 变成 6, 5 变成 3, 6 变成 7, 7 变成 4, 8 仍然是 8. 用循环记号来写就是 $(1)(2\,5\,3)(4\,6\,7)(8)$. 循环形是 $(3^2, 1^2)$, 所以它的阶是 3 和 1 的最小公倍数, 就是 3]. 所以, 像这样洗牌 3 次以后, 牌就都回到了自己原来的位置. 如果牌的张数不同, 问题可以变得更有趣, 您可能愿意用 52 张牌自己试一试.

置换还有一个比较微妙的方面, 对于群论是有意义的, 就是**偶**和**奇置换**的理论. 最好仍然是用例子来说明它. 取 $n = 3$, 而令 x_1 , x_2 , x_3 为 3 个变量. 现在把 S_3 中的置换设想为这 3 个变量在互变, 而不是 3 个数 1, 2 和 3 在互变. 例如, 以 $(1\,3\,2)$ 来表示 x_1 变为 x_3, x_3 变为 x_2, 而 x_2 变为 x_1. 现在令 $\Delta = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$. S_3 中的置换以一种显然的方式作用于 Δ 上, 例如 $(1\,2\,3)$ 把 Δ 变为 $(x_2 - x_3)(x_2 - x_1)(x_3 - x_1)$.注意这恰好就是 Δ, 不过有两个括号改变了其中各项的先后: $(x_1 - x_2)$ 和 $(x_1 - x_3)$, 所以 $(1\,2\,3)$ 把 Δ 仍变为 Δ. 但是, 若以 $(1\,2)(3)$ 作用于 Δ, 就会得到 $(x_2 - x_1)(x_2 - x_3)(x_1 - x_3) = -\Delta$. 可以看到, S_3 中的置换把 Δ 要么变成 Δ, 要么变成 $-\Delta$. 我们把变 Δ 为 Δ 的称为**偶置换**, 而把变 Δ 为 $-\Delta$ 的称为**奇置换**. 请验证, ι , $(1\,2\,3)$ 和 $(1\,3\,2)$ 都是偶置换, 而 $(1\,2)(3)$, $(1\,3)(2)$ 和 $(2\,3)(1)$ 都是奇置换.

对于一般的 n, 偶置换和奇置换的定义很相似于上面的例子. 令 $x_1, \cdots, x_n$ 是变量, 而 S_n 中的置换是把这些变量互变, 而不是把 $1, 2, \cdots, n$ 这些标号互变. 定义 Δ 为所有的 $x_i - x_j$ 的乘积, 不过, 这时规定 $i < j$: $\Delta = \prod_{i<j}(x_i - x_j)$[①] . 把 $g \in S_n$ 作用于 Δ, 或者得到 Δ, 或者得到 $-\Delta$. 定义 g 的**符号**[②] 为一个数

① 这个函数时常被称为交错函数, 请参看下文关于交错群的定义. —— 中译本注

② signature 一词在数学中有多个用法. 最常见的是用于实二次型理论 (就是实对称矩阵的理论) 中, 指正本征值的个数与负本征值的个数之差, 因此常译为 "符号差". 但是在置换理论中, 并没有 "差" 的意思, 而仅仅是指 Δ 在一个置换下的符号变化与否. 所以, 我们在这里直接译为符号. —— 中译本注

$\mathrm{sgn}(g) \in \{+1, -1\}$, 使得 $g(\Delta) = \mathrm{sgn}(g)\Delta$. 这样就定义了符号函数 $\mathrm{sgn}: S_n \to \{+1, -1\}$. 于是, S_n 中的置换 g 称为偶置换, 如果 $\mathrm{sgn}(g) = +1$; 称为奇置换, 如果 $\mathrm{sgn}(g) = -1$.

由定义很容易得知, 对于任意的 $g, h \in S_n$,

$$\mathrm{sgn}(gh) = \mathrm{sgn}(g)\,\mathrm{sgn}(h),$$

也容易得到, 任意 2 循环的符号为 -1. 对于 r 循环, 因为 $(a_1\, a_2\, \cdots\, a_r) = (a_1\, a_r)(a_1\, a_{r-1})\cdots(a_1\, a_2)$, 所以 r 循环的符号是 $(-1)^{r-1}$. 因此循环形为 $(r_1, r_2, \cdots, r_k)$ 的置换 $g \in S_n$ 的符号是

$$\mathrm{sgn}(g) = (-1)^{r_1-1}(-1)^{r_2-1}\cdots(-1)^{r_k-1}.$$

这就使得任意置换的符号都很容易算出来. 例如, S_5 中的偶置换就是循环形为 (1^5), $(2^2, 1)$, $(3, 1^2)$ 或 (5) 的那些置换. 如果计算一下, 就会知道总共有 60 个偶置换, 恰好是置换总数 $5! = 120$ 的一半. 一般说来, S_n 中的偶置换为数 $\frac{1}{2}n!$.

这个复杂的定义意图何在? 答案是, S_n 中的偶置换构成一个大小为 $\frac{1}{2}n!$ 的子群, 称为 ***n* 次交错群**, 记作 A_n. 交错群是很重要的有限群的例子, 这是由于以下的事实: 当 $n \geqslant 5$ 时, A_n 是单群, 即只以恒等群以及 A_n 本身为*正规子群*[I.3 §3.3] 的群 (见条目*有限单群的分类*[V.7]), 例如 A_5 是大小为 60 的单群. 事实上, 它是最小的非阿贝尔有限单群.

III.69 相 变

(Phase Transitions)

如果把一块冰加热, 它就会变成水. 这个人们很熟悉的现象其实很神秘, 因为它表明, 化学化合物 H_2O(水) 的性质并不是连续依赖于温度的, 一块冰直接从固态变为液态, 而不需要经过一个逐渐变软的过程.

这就是**相变**的一个例子. 在有大量具有 "局部" 的相互作用的粒子族中, 总会发生相变. 这里的局部相互作用就是说一个粒子的性态, 只受到其直接紧邻的粒子的影响.

可以作出这种系统的数学模型, 而这种模型的研究, 属于所谓**统计物理学**的领域. 对于这种模型的进一步讨论, 可见条目*临界现象的概率模型*[IV.25].

III.70 π

从数学上说, 是什么使得一个数比其他的数更为基本、更为重要? 例如, 为什么几乎每一个人都会认为 2 比 $\frac{43}{32}$ 更加重要? 一个可能的回答是, 关于一个数, 真正起作用的是它的性质, 特别是它可能具有的有趣的性质, 使它与别的数区别开来. 当然, 这就要求我们来决定什么算是有趣的性质, 例如, $\frac{43}{32}$ 是唯一的加倍以后成为 $\frac{43}{16}$ 的数, 为什么这不算是有趣的性质呢? 一个明显的理由是, 每一个您打算取的数, 都有可以与此类比的性质: x 是唯一的加倍以后成为 $2x$ 的数. 对照起来, "是最小素数" 这个性质, 并未提出任何特定的数, 而且很容易用一个概念 "素数" 来陈述, 而这个概念本身的重要性又容易解释. 这个性质讲的恰好是一个数, 而这个数很可能在数学中起重要的作用. 事实上也就是这样 (巧的是, 据猜测, $\frac{43}{32}$ 也是统计物理学里一个重要的临界指数, 所以也可以把它举出来, 作为有趣的数, 但是它仍然不能如 2 那样基本).

每个人都会同意, π 是数学中最重要的数之一, 也很容易用前面提出的判据来论证这一点, 因为 π 有许许多多性质 —— 性质之多, 使它时常在计算中不经意地出现, 使人吃惊也不为过. 例如, 下面就是欧拉[VI.19] 的著名定理:

$$\sum_{n=1}^{\infty}\frac{1}{n^2}=1+\frac{1}{4}+\frac{1}{9}+\frac{1}{16}+\frac{1}{25}+\cdots=\frac{\pi^2}{6}.$$

人们可能奇怪, π 到底与完全平方数的倒数之和有什么关系呢? 这是一个完全有道理的问题, 但是对于一个有经验的数学家, 二者从原则上说有关系并不使人吃惊. 证明一个恒等式的一个很普通的方法, 就在于说明等式双方其实是估计同一个量的不同方法. 在我们这个情况, 可以利用傅里叶分析[III.27] 的一个基本的结果, 称为普兰舍利恒等式, 它指出了以下的事实: 如果 $f:\mathbf{R}\to\mathbf{C}$ 是一个以 2π 为周期 [且在一个周期内平方可积] 的周期函数, 而对 (正或负) 整数 n 定义其第 n 个傅里叶系数[①] a_n 为

$$a_n=\frac{1}{2\pi}\int_{-\pi}^{\pi}f(x)\mathrm{e}^{-inx}\mathrm{d}x,$$

这时

$$\frac{1}{2\pi}\int_{-\pi}^{\pi}|f(x)|^2\mathrm{d}x=\sum_{n=-\infty}^{\infty}|a_n|^2.$$

① 本书条目 [III.27] 指出, 傅里叶系数与傅里叶变换的写法在各书中常有不同, 因此许多结论的形式也会稍有区别. 译者也指出了我国常用的教材所用的写法, 本文中使用的记号即与国内常用的一致. 所以, 下面普兰舍利公式左方积分前有一个因子 1/2π, 而 [III.27] 中的公式则没有这个因子. 又, 本文 a_n 的积分号下的因子, 原书误为 e^{inx}, 与原书其他用到这个公式的地方都有矛盾, 这里改过来了. —— 中译本注

若令 f 是这样的周期函数：它在 [每一个周期之内], 在区间 $\left[-\frac{\pi}{2}, \frac{\pi}{2}\right]$ 里值为 1, 这里 n 是一个整数, 而在其余地方 $f=0$, [然后对它以 2π 为周期, 取周期拓展], 则上式左方容易计算出来等于 $\frac{1}{2}$. 稍作计算又可以得到, 当 n 为奇数时, $|a_n|^2 = 1/(n\pi)^2, |a_0|^2 = \frac{1}{4}$, 而当 n 为非零偶数时, $|a_n|^2 = 0$. 所以

$$\frac{1}{2} = \frac{1}{4} + \frac{1}{\pi^2} \sum_{n\text{为奇}} \frac{1}{n^2}.$$

注意到 $n^2 = (-n)^2$, [所以上式右方的和号包含了两个相等的部分, 即分别对 n 为正的或负的奇数求和]. 这样, 化简以后有

$$\frac{\pi^2}{8} = 1 + \frac{1}{3^2} + \frac{1}{5^2} + \frac{1}{7^2} + \cdots.$$

它与我们想要证明的结果已经很相像了, 如果再注意到此式右方可以写为 $\sum_n \frac{1}{n^2} - \sum_n \frac{1}{(2n)^2} = \frac{3}{4} \sum_n \frac{1}{n^2}$, 就立刻有 $\sum_n \frac{1}{n^2} = \frac{\pi^2}{6}$.

现在我们对于 π 的出现找到了一个理由, 它的出现是由于在傅里叶系数公式里面就有它, 它在那里出现也可以解释. 定义在 $\mathbf{R}$ 上的周期函数, 看作是定义在单位圆周上的函数更为自然. 傅里叶系数是在单位圆周上的某种平均值, 所以应该用单位圆周的长度 2π 去除.

那么, π 到底是什么呢? 我们刚才看到的大概是它的最简单的定义了: 它是圆周长和直径之比. 但是, 使得 π 如此有趣的是有许多性质可以作为它的定义, 下面略举几个.

(i) 定义 $\sin x$ 为以下幂级数之和

$$x - \frac{x^3}{3!} + \frac{x^5}{5!} - \cdots,$$

则 π 是使得 $\sin x$ 为 0 的最小正数 (关于 $\sin x$, 详见条目三角函数[III.92]).

(ii) $\pi = \int_{-1}^{1} \frac{\mathrm{d}x}{\sqrt{1-x^2}}$.

(iii) $\frac{\pi}{2} = \int_{-1}^{1} \sqrt{1-x^2}\,\mathrm{d}x$.

(iv) $\frac{\pi}{4} = \left(1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \cdots\right)$.

(v) $\sqrt{2\pi} = \int_{-\infty}^{\infty} \mathrm{e}^{-x^2}\,\mathrm{d}x$.

(vi) $\pi=\sum_{k=0}^{\infty}\frac{1}{16^k}\left(\frac{4}{8k+1}-\frac{2}{8k+4}-\frac{1}{8k+5}-\frac{1}{8k+6}\right)$.

第二和第三个性质右方的积分分别是单位圆的半周长和半圆面积, 所以这两个性质是单位圆周长为 2π 和面积为 π 这些几何事实的分析表示.

第五个性质告诉我们, 在 $e^{-x^2/2}$ 前面要附上什么常数才能使它成为著名的正态分布[III.71 §5](为什么 π 又进来了? 可以找到好几个理由, 其中之一是, 函数 $e^{-x^2/2}$ 在傅里叶分析中起特殊的作用, π 也起特殊作用, [所以二者就有了联系]. $e^{-x^2/2}$ 的另一个基本的性质是函数 $f(x,y)=e^{-(x^2+y^2)/2}$ 具有旋转不变性, 旋转既然涉及圆, 自然也就涉及 π).

最后的性质是 David Bailey, Peter Borwein 和 Simon Plouffe 新近的值得注意的发现. 因子 $1/16^k$ 的出现给出了计算 π 的 16 进制 (即以 16 为底的小数) 表示的一种方法, 其中不必先算出前面的数码. 它被用来算出在 16 进制表示中远得惊人的位置处的数码, 例如, 已经算出其万亿分位的十六进数码是 8(条目数学: 一门实验科学[VIII.5 §7] 中有关于这个公式的进一步的讨论).

对于非数学家来说, 像 π 这样自然的数, 竟然是无理数, 甚至超越数, 简直是近乎悖论[III.41] 了. 但是这完全不奇怪: 定义 π 的性质是很简单的, 但是不会引导到多项式方程的解. 所以, 如果 π 不是超越数, 那倒反而怪了. 类似地, 如果在 π 的十进小数展开式里面能够找到数码排列的特别的模式, 那将是一个很大的惊奇. 实际上, 现在人们猜想, π 对于底 10 是正常的, 意思是在这个展开式里, 任何一串数码出现的频率都正如您的设想. 例如, 如果您想看连续两位数码, 就会期望到 35 出现的频率大概是百分之一. 但是, 这个猜测好像很困难, 甚至连在 π 的十进小数展开中, 0 到 9 这 10 个数码都会出现无穷次, 都还没有证明.

III.71 概率分布 (Probability Distributions)

James Norris

1. 离散分布

当投掷一枚硬币时, 我们对于它将会哪一面向上毫无所知. 但是在一个不同的意义下, 硬币的行为又是高度可预测的: 如果投掷多次, 则正面向上的次数之比, 会很接近 $\frac{1}{2}$.

为了从数学上来研究这种现象, 需要先建立模型, 它是这样做的: 首先是定义样本空间, 就是可能的结果的集合, 再在这个空间上定义概率分布, 说明这些可能

结果的概率. 在投掷硬币的例子里, 自然的样本空间就是集合 $\{H,T\}$, 而一个明显的概率分布, 是对样本空间的这两个元素各赋以概率 $\frac{1}{2}$. 换一个写法, 因为我们感兴趣的是正面出现的次数, 所以就把投掷的结果用 $\{0,1\}$ 来表示: 每一次投掷以后, 正面出现的次数为 0 的概率是 $\frac{1}{2}$, 出现次数为 1 的概率也是 $\frac{1}{2}$. 更一般的情况是, 一个 (离散的) 样本空间就是一个集合 Ω, 其上的概率分布就是对 Ω 的每一个元素赋给一个非负实数的方法, 使得这些实数之和为 1. 赋给一个元素的实数就解释为相应结果出现的概率, 而总概率为 1.

如果 Ω 的大小为 n, Ω 上的均匀分布就是对 Ω 的每一个元素都指定概率 $1/n$ 的概率分布. 然而, 对于 Ω 的不同的元素赋予不同的概率可能更适当. 例如, 给定一个 0 和 1 之间的实数 $p : 0 \leqslant p \leqslant 1$, 对集合 $\{0,1\}$ 中的 1 赋予概率 p, 而对 0 赋予概率 $1-p$, 这个概率分布称为参数为 p 的伯努利分布 ①. 它可以用来作为投掷偏心硬币的模型.

现在设投掷一个不偏心的硬币 n 次. 如果我们关心的是每一次投掷的结果, [这个结果可以写成长度为 n 的由 0 和 1 组成的序列. 这种序列的集合就是我们需要的样本空间]. 举例来说, 如果 $n=5$, 那么 01101 就是这个样本空间的典型元素 (它表示投掷的结果依次是反、正、正、反、正). 因为这样的序列共有 2^n 个, 而且看来每一种结果的出现都是机会均等的, 那么, 对每一个序列就应该赋予概率 $1/2^n$.

如果我们关心的不是特定的正面、反面序列, 而是在 n 次投掷中正面出现的总次数, 那么又该怎么办呢? 这时, 样本空间就是集合 $\{1,2,\cdots,n\}$. 正面出现的总次数为 k 的概率就应该是 2^{-n} 乘上在 01 序列中出现 k 个 1 的这一类序列的总数. 这个数就是

$$\begin{pmatrix} n \\ k \end{pmatrix} = \frac{n!}{k!(n-k)!},$$

所以对于样本空间中的元素 k 所赋予的概率是 $p_k = \begin{pmatrix} n \\ k \end{pmatrix} 2^{-n}$.

一般的情况是: 如果做 n 次独立的试验, 而每一次成功的概率都同为 p, 失败的概率则为 $1-p$, 那么在这 n 次试验中有指定的 k 次成功, 而其余 $n-k$ 次失败, [出现这种成功和失败的特定序列] 的概率就是 $p^k(1-p)^{n-k}$; 而 n 次试验中恰好有 k 次成功 (不论是哪 k 次) 的概率则是 $p_k = \begin{pmatrix} n \\ k \end{pmatrix} p^k(1-p)^{n-k}$. [现在, 样本空间仍然是集合 $\{1,2,\cdots,n\}$, 而上面给出的概率分布]称为参数为 p 与 k 的二项分布, 它就是投掷偏心的硬币 n 次的模型.

① 这里是指雅各布 · 伯努利, 见伯努利家族[VI.18].—— 中译本注

假设无限地进行上面的试验, 直到出现第一次成功为止. 如果是在第 k 次成功, 而前 $k-1$ 次失败, 这种情况出现的概率是 $p_k=(1-p)^{k-1}p$. 所以, [当 k 变动时], 它给出了首次成功是第 k 次的概率. 这也是一个概率分布, 称为参数为 p 的几何分布. 特别是投掷公平的硬币, 在某一次首次出现正面的概率分布就是参数为 $\frac{1}{2}$ 的几何分布. 现在的样本空间 [则是 $\{1,2,\cdots,n,\cdots\}$], 是一个无限集合, 而这时概率之和为 1 的条件应该写成 $\sum_{k=1}^{\infty}p_k=\sum_{k=i}^{\infty}(1-p)^{k-1}p=1$. [它实际上是成立的, 因为

$$\sum_{k=1}^{\infty}(1-p)^{k-1}p=p\sum_{l=0}^{\infty}(1-p)^{l}=p\cdot\frac{1}{1-(1-p)}=1].$$

现在考虑一个比较复杂的试验, 设有一个放射源, 随时会因衰变而发射出一个 α 粒子. 假设这些衰变是独立事件, 则下面的假设是合理的, 即在任何时刻衰变的机会都是均等的. 如果每分钟平均的衰变次数例如是 λ, 那么在给定的任意一分钟内, 因衰变而发射出 k 个粒子的概率是多少?

考虑这个问题的方法之一是把一分钟分成大小相同的 n 个区段, 这里 n 是一个很大的数, 那么在一个区段里发射了两个粒子的概率是如此的小, 而可以忽略, 所以既然每一分钟衰变的次数平均是 λ, 则在任何一个区段里发生衰变, 因而发射一个粒子的概率是 λ/n, 记次数为 p. 因为衰变是互相独立的, 所以可以把衰变次数看成 n 次试验中成功的次数, 而每一次成功的概率都是 p. 这样就会得到一个参数为 n 和 p 而 $p=\lambda/n$ 的二项分布.

注意, 当 n 变大时, p 就会变小, 而上面做到近似也就更好. 因此自然会令 $n\to\infty$, 而来研究所得的 "极限分布". 可以证明, 当 $n\to\infty$ 时, 二项分布的概率的极限是 $p_k=\mathrm{e}^{-\lambda}\lambda^k/k!$. 这些数在非负整数 (就是 k) 的集合上定义了一个概率分布, 称为参数为 λ 的泊松分布.

2. 概率空间

假设向靶子投掷一支镖. 因为投手不甚长于此道, 所以对于镖会射中靶上的何处, 不能说得很清楚, 但是至少可以用概率方法做一个模型. 很明显, 样本空间就是一个圆盘, 盘中的点就是镖射中之处. 然而, 现在有了一个问题, 如果瞄准靶上的一个特定的点, 则镖恰好射中此点的概率为 0. 那么, 该怎样定义概率分布?

回答这个问题的线索在于这样一件事, 下面的问题完全容易说明其意思: "射中牛眼①(bullseye) 的概率是多少?" 要想射中牛眼, 镖就必须命中靶的一定区域, 而发生这种事的概率当然不必是 0. 例如, 它可能是牛眼的面积除以靶的总面积.

①靶的中心部分, 其半径规定约为 13mm.—— 中译本注

我们所看到的事就是, 哪怕不能对样本空间的个别的点指定其概率, 我们仍然希望对其子集合给出其概率. 这样, 若样本空间是 Ω, 而 A 是 Ω 的子集合, 则可以试着对 A 指定 0 与 1 之间的一个数 $P(A), 0 \leqslant P(A) \leqslant 1$. $P(A)$ 就表示随机的结果属于子集合 A 的概率, 可以把这个概率看作是一个类似于 A 的 "质量" 的概念.

为了使这样做能解决问题, 需要令 $P(\Omega)=1$(就是说, 在样本空间总会发生什么事情, 所以发生各种情况的总的概率为 1). 还有, 如果 A 和 B 是 Ω 的两个分离的子集合, 则 $P(A \cup B)=P(A)+P(B)$. 由此得到, 如果子集合 $A_1, \cdots, A_n$ 都是互相分离的, 则有下式成立: $P(A_1 \cup \cdots \cup A_n)=P(A_1)+\cdots+P(A_n)$. 事实证明了重要的是要求此式不仅对于有限并成立, 而且对可数个[III.11] 子集合的并也成立 (与此相关的一个事实是, 我们并不打算对 Ω 的一切子集合 A 都来定义 $P(A)$, 而只需要对它的一切可测子集合[III.55] A 来定义 $P(A)$, 而在我们的情况下, 只要能对实际上能够定义的 A 来定义 $P(A)$ 也就够了).

一个概率空间就是一个样本空间以及定义在所有 "合乎情理的" 子集合上的满足前两段中提出的条件的函数 P. P 本身称为一个概率测度或概率分布, 而当具体地确定 P 时, 概率分布这个词用得较多.

3. 连续的概率分布

有三个特别重要的定义在 $\mathbf{R}$ 上的概率分布, 本节中只讨论其中两个. 第一个是定义在区间 $[0,1]$ 上的均匀分布. 我们很愿意精确地刻画 "$[0,1]$ 中的所有点都同等可能" 这个思想, 但是由于上面已经提出的一个点的概率可能为 0 的问题, 这件事怎样去做呢?

一个好办法是认真地看待 "质量" 这个比喻. 虽然我们不能通过计算一个物体的无穷小的点的质量并把它们相加来求这个物体的质量, 但可以对这些点指定密度, 然后对密度进行积分, 在这里就是要这样做. 在均匀分布的情况下, 对 $[0,1]$ 中的每一个点都指定一个概率密度 1, 然后定义一个子区间, 例如 $\left[\frac{1}{3}, \frac{1}{2}\right]$ 的概率为一个积分: $P([1/3,1/2])=\int_{1/3}^{1/2} 1 \mathrm{d}x=\frac{1}{6}$. 一般说来, 子区间 $[a, b] \subset [0,1]$ 的概率就是其长度 $b-a$. [这样规定了概率以后, 可数多个互相分离的子区间的并] 的概率当然就等于各个小区间的概率之和, [而整个样本空间 $[0,1]$ 的总概率自然为 1. 这样, 对于概率分布的要求都得到了满足].

这个 "连续的" 均匀分布, 也和它的离散的均匀分布一样, 有时可以从对称性的要求自然地出现, 它也可以作为一个极限分布而出现. 假设有一位隐士, 身居洞穴之内而不见天日, 也没有钟表, 他的 "一天" 的长度, 可以随机地在 23 个小时到 25 个小时之间. 一开始, 他还可能有一点时间的概念, 他可以说这样的话: "我才吃

了午饭, 外边大概天亮了吧", 但是, 时间流逝, 过了几个星期, 他已经完全没有了这样的时间概念, 对于他, 说外界的时间是几点钟, 都是一样的: [是早晨、黄昏, 概率完全一样].

现在来考虑一个有趣得多的密度函数, 它依赖于一个正常数的选择, 这就是定义在所有非负实数集合上的密度函数 $f(x) = \lambda e^{-\lambda x}$. [现在, 样本空间是 $[0,\infty)$]. 为了作出 $[0,\infty)$ 的子区间 $[a,b]$ 的概率, 我们用下面的积分算出:

$$\int_a^b f(x)\,dx = \int_a^b \lambda e^{-\lambda x}dx = e^{-\lambda a} - e^{-\lambda b}.$$

[当然, 关于概率所应该满足的条件如可数可加性和 $P(\Omega) = P([0,\infty)) = 1$ 都得到满足]. 所得的概率分布称为参数为 λ 的指数分布. 如果要为自发发生的事件的发生时间 T, 如放射性核的衰变的发生时间, 构造一个数学模型, 还有下一封垃圾电子信件到达时间的数学模型, 指数分布就是适用的, 其所以如此的理由在于无记忆性. 例如, 设已经知道一个放射性核在时刻 s 之前没有动静, 那么, 它在以后的时刻 $s+t$ 发生衰变的概率和它从初始时刻一直到时刻 t 才衰变的概率是一样的. 令 $G(t)$ 表示在时刻 t 才初次衰变的概率, 于是, [它的衰变发生在时刻 s 和时刻 $s+t$ 之间的概率] 应该是 $G(s+t)/G(s)$, 而这又应该等于 $G(t)$. 与此等价, 有 $G(s+t) = G(s)G(t)$. 唯一具有这个性质的下降函数是**指数函数**[III.25], 也就是形如 $G(t) = e^{-\lambda t}$ 的函数, 这里 λ 是一个正数. 因为 $1-G(t)$ 表示衰变发生在区间 $[0,t]$ 中的概率, 如果发生这一事件的概率密度是 $f(t)$, 则由概率密度的定义, 可以得出 $1-G(t) = \int_0^t f(x)\,dx$, 所以 $f(t) = \lambda e^{-\lambda t}$.

下一节要开始讲第三个也是最重要的一个概率分布.

4. 随机变量, 平均值和方差

给定一个概率空间, 定义事件就是这个空间的一个 "充分好" 的子集合. 例如, 设概率空间为区间 $[0,1]$ 以及其上的均匀分布, 则区间 $\left[\frac{1}{2},1\right]$ 就是这样一个事件: 它代表随机取出的一个数至少是 $\frac{1}{2}$. 不仅要思考一个随机事件, 而且思考与一个概率空间相关联的随机的数, 这时常是很有用的. 例如, 再次看一下投掷一个偏心的硬币的试验序列, 而设投掷这个硬币时正面向上的概率为 p. 与这个试验相关的自然的样本空间是所有的由 0 和 1 组成的序列的集合 Ω. 在前面说明了 [在 n 次试验中], 得到 k 次正面的概率是 $p_k = \binom{n}{k} p^k(1-p)^{n-k}$, 那时, 我们是取 $\{0,1,\cdots,n\}$ 为样本空间, 而取 p_k 为概率分布的. 然而, 在许多方面都更加自然而且远为更加有

用的是取这里的 Ω 为样本空间, 而来定义其上的一个函数 $X:\Omega\to\mathbf{R}$, 表示正面向上的次数, 就是说, $X(\omega)$ 表示序列 ω 中有多少个 1. 这时, 就可以写出

$$P(X=k)=p_k=\binom{n}{k}p^k(1-p)^{n-k}.$$

一个像这样的函数就称为一个随机变量. 如果 X 是一个在集合 Y 中取值的随机变量, 则 X 的分布就是按下式定义在 Y 的子集合 A 上的函数 P:

$$P(A)=P(X\in A)=P(\{\omega\in\Omega:X(\omega)\in A\}).$$

不难看到, 函数 P 就是 Y 上的一个概率分布.

在许多时候, 只需要知道一个随机变量的分布. 但是, 对于在一个样本空间上的随机变量的概念, 包含了我们关于一个随机量的直觉, 而且使我们能问许多进一步的问题. 例如我们想要在下面的条件下求 [在 n 次投掷中] 出现 k 个正面的概率, 条件是第一次和最后一次投掷的结果是相同的, 这时, 只是 X 的分布是不够的, 但是更丰富的视 X 为定义在所有序列的集合 [即样本空间 Ω] 上的函数, 这个模型就行. 此外, [这个更丰富的模型] 还使得我们可以讨论所谓独立的随机变量 $X_1,\cdots,X_n$, 其意义就是要求 Ω 的适合以下的条件的元素 ω: 对于所有的 i 均有 $X_i(\omega)\in A_i$, 对于所有的乘积 $A_1\times\cdots\times A_n$, 这种 ω 所成的子集合 $\{\omega:X_i(\omega)\in A_i,i=1,2,\cdots,n\}$ 的概率都等于乘积 $P(X_1\in A_1)\times\cdots\times P(X_n\in A_n)$.

有两个重要的数可以从一开始起就用来刻画一个随机变量 X, 就是它的平均值或称期望值 $E(X)$ 和方差 $\operatorname{var}(X)$, 二者都可以用 X 的分布来定义. 如果 X 只取整数值, 而且其分布是 $P(X=k)=p_k$, 则定义

$$E(X)=\sum_k kp_k,\quad \operatorname{var}(X)=\sum_k(k-\mu)^2p_k,\quad \mu=E(X).$$

平均值告诉我们 X 平均有多大. 方差或者更好是它的平方根, 即所谓标准差 (standard deviation) $\sigma=\sqrt{\operatorname{var}(X)}$, 则告诉我们 X 偏离其平均值典型地有多远. 不难导出方差的另一个有用的公式

$$\operatorname{var}(X)=E(X^2)-E(X)^2.$$

为了更好地理解方差的意义, 看下面的情况: 设有 100 位考生参加一场考试. 满分是 100, 而他们的平均分是 75. 这个数据给了一些信息, 但远非分数分布的完全的情况. 例如, 可能共有四个考题, 其中三个非常容易, 而另一个难得几乎谁也做不出来, 所以绝大部分的考分都聚集在 75 分左右; 但也可能是 50 个学生得了满分, 而另外 50 个只得了 50 分. 为了做出考试结果的模型, 设样本空间 Ω 就是这 100 位考生. 给定了一个随机的考生 ω, 记其得分是 $X(\omega)$, 则在概率分布是均匀分布的

第一个情况下, 方差会很小, 因为每一个人的得分都很接近于 75 分的平均分. 而在第二个情况下, 方差很接近 $25^2 = 625$, 因为每个人的分数都离 75 分的平均值达到 25 分之多. 方差就能帮助我们了解这两种情况的差别.

正如本文开始时提到的, 我们的经验是, 投掷一个公正的硬币 n 次, 我们所能 "期望" 得到的正面向上的次数是 $n/2$, 就是说, 出现正面的比通常近于 $1/2$. 不难算出, 若用 X 来模拟 n 次投掷中出现正面的次数, 而 X 服从参数为 n 和 $1/2$ 的二项分布, 则 $E(X) = \frac{1}{2}n$, 而方差 $\operatorname{var}(X) = \frac{1}{4}n$, 所以自然地量度分布的分散程度的是标准差 $\sigma = \frac{1}{2}\sqrt{n}$. 稍作计算就知道, 对于很大的 n, X/n 以接近 1 的概率接近于 $\frac{1}{2}$. 这些计算与我们的经验都是相符的.

一般地说, 设 $X_1, X_2, \cdots, X_n$ 是独立的随机变量, 则它们的和的方差等于各个随机变量的方差的和: $\operatorname{var}(X_1 + \cdots + X_n) = \operatorname{var}(X_1) + \cdots + \operatorname{var}(X_n)$. 由此可知, 如果所有的 X_i 都有相同的概率分布、相同的平均值 μ、相同的方差 σ^2, 则样本平均值 $\tilde{X} = n^{-1}(X_1 + \cdots + X_n)$ 的方差是 $n^{-2}(n\sigma^2) = \sigma^2/n$[①], 所以当 $n \to \infty$ 时, 趋于 0. 这一点观察可以用于证明, 当 $n \to \infty$ 时, $|\tilde{X} - \mu|$ 大于 $\varepsilon\,(\varepsilon > 0)$ 的概率趋于 0, 这里 ε 是任意正数. 所以, 样本平均值 "依概率收敛" 于平均值 μ.

这个结果称为弱大数定律. 上面概述的论证中隐含地假设了这些随机变量具有有限的方差, 而后来证明, 这个假设实际上是不必要的. 还有一个强大数定律, 它指出, 当 $n \to \infty$ 时, 前 n 个随机变量的样本平均值以概率 1 收敛于 μ. 顾名思义, 强大数定律比弱大数定律更强, 意思是从强大数定律可以导出弱大数定律. 注意, 这些定律使得我们可以对那些用概率理论作模型的实际事件作出一种统计性质的长期预报. 此外, 这些预报是可以用实测来验证的, 而试验数据确实证实了它们, 这就给我们的模型以能够服人科学依据.

5. 正态分布与中心极限定理

我们已经看到, 参数为 n 和 p 的二项分布的概率是由公式 $p_k = \binom{n}{k} p^k (1-p)^{n-k}$ 给出的. 如果 n 很大, 把点 (k, p_k) 描成一个图, 就会得到一个钟形的曲线, 它在平均值 np 处有一个很尖的峰值. 这个曲线高耸部分的宽度的数量级有如标准差 $\sqrt{np(1-p)}$. 为简单计, 设 np 是一个整数, 并且定义一个新的概率分布 $q_k = p_{k+np}$. 于是, 新的曲线峰值移到了 $k = 0$ 处. 如果再把这个图形的比例改变, 水平方向按因子 $\sqrt{np(1-p)}$ 压缩, 而垂直方向则按因子 $\sqrt{np(1-p)}$ 拉伸, 这样, 原来的点都位于函数

①原书分母误为 $2n$, 这里改成 n. —— 中译本注

$$f(x)=\frac{1}{\sqrt{2\pi}}\mathrm{e}^{-x^2/2}$$

的图像附近. 这是一个著名的分布, 即 $\mathbf{R}$ 上的标准正态分布的分布函数. 它也称为高斯分布.

换一个不同的说法, 如果投掷一个偏心的硬币很多次, 然后从正面出现的次数减去其平均值, 再除以标准差, 就会接于一个标准正态分布.

函数 $\mathrm{e}^{-x^2/2}/\sqrt{2\pi}$ 出现在许多数学分支里, 从概率论到傅里叶分析[III.27]、到量子力学里面都可以找到它. 为什么会这样? 和许多这一类问题相同, 答案是这个函数具有一些其他函数所没有的性质.

这类性质之一是它的旋转不变性. 假设再一次瞄着靶子上的牛眼掷出一支镖. 可以把两个在互相垂直方向上独立的正态分布加起来作为其模型: 一个正态分布是 x 方向的模型, 另一个是 y 方向的, 而且设二者都有平均值 0 和方差 1. 如果这样做, 那么 2 维的密度函数将是 $(1/2\pi)\,\mathrm{e}^{-x^2/2}\mathrm{e}^{-y^2/2}$, 它可以方便地写成 $(1/2\pi)\,\mathrm{e}^{-r^2/2}$, r 表示由原点到 (x,y) 的距离. 换句话说, 密度函数只依赖于到原点的距离 (这就是为什么称它为 "旋转不变的"). 这个非常吸引人的性质在高维情况下也成立. 可以证明, $(1/2\pi)\,\mathrm{e}^{r^2/2}$ 是唯一具有这个性质的函数, 就是说, 它是唯一的旋转不变而且其坐标 x 和 y 是独立的方差为 1 的随机变量的密度函数. 这样, 正态分布具有非常特别的对称性质.

像这样的性质, 使得我们在解释正态分布在数学中无处不在方面走了一大步. 然而正态分布还有一个甚至更加值得注意的性质, 使得当用数学建立现实世界的无序性的模型时, 正态分布总会出现. 中心极限定理指出, 对于任意独立的而且具有相同分布的随机变量的序列: $X_1,X_2,\cdots$(它们的平均值都是有限的 μ, 方差也是相同的 σ^2), 则对任意实数 x 总有

$$\lim_{n\to\infty}P\left(X_1+\cdots+X_n\leqslant n\mu+\sqrt{n}\sigma x\right)=\int_{-\infty}^{x}\frac{1}{\sqrt{2\pi}}\mathrm{e}^{-y^2/2}\mathrm{d}y.$$

$X_1+\cdots+X_n$ 的期望值是 $n\mu$, 标准差是 $\sqrt{n}\sigma$, 所以思考这个问题又可以换一个角度: 令 $Y_n=(X_1+\cdots+X_n-n\mu)/\sqrt{n}\sigma$, 这样把随机变量 X_i 重新尺度化为 Y_n, 则 Y_n 的平均值成为 0, 而方差成为 1, 而上面的概率就变成了 $Y_n\leqslant x$ 的概率. 这样, 不论从什么样的分布开始, 在适当地重新尺度化以后, 许多同样的随机变量之和的极限分布总是正态分布. 许多自然过程都可以很合乎实际地以大量微小的独立随机效应的聚集为其数学模型. 这就是为什么我们所观察到的许多分布, 如某个城市里成人身高的分布等等, 都是我们熟悉的钟形曲线.

中心极限定理有一个很有用的应用, 就是它可以用于简化一些几乎无法处理的复杂计算. 例如, 二项分布概率的计算, 当参数 n 很大时, 复杂得几乎令人束手无策. 但是, 如果 X 是一个二项随机变量, 设其参数例如为 n 和 $1/2$, 则可以把 X 写

为一个和 $Y_1+\cdots+Y_n$, 而 $Y_1,\cdots,Y_n$ 是独立的参数为 1/2 的伯努利随机变量. 于是, 由中心极限定理有

$$\lim_{n\to\infty} P\left(X \leqslant \frac{1}{2}n+\frac{1}{2}\sqrt{nx}\right)=\int_{-\infty}^{x}\frac{1}{\sqrt{2\pi}}\mathrm{e}^{-y^2/2}\mathrm{d}y.$$

III.72 射 影 空 间
(Projective Space)

实射影平面可以用不同的方法来定义. 方法之一的用三个齐次坐标: 一个典型的点表示为 (x,y,z), 其中 x,y 和 z 不同时为 0, 而且还规定: 若 λ 是一个非 0 实常数, 则 (x,y,z) 和 $(\lambda x,\lambda y,\lambda z)$ 要看成相同的点. 注意到在 3 维空间 $\mathbf{R}^3$ 中, 对于每一组 (x,y,z), 所有形如 $(\lambda x,\lambda y,\lambda z)$ 的点构成一条通过原点和 (x,y,z) 点的直线, 所以实射影平面的更加有几何味儿的定义是: 它就是过原点的直线的集合. 每一条这样的直线与单位球面恰好交于两个对径点 (即一条直径的两个端点), 所以实射影平面的第三个定义就是: 视单位球面的每一对对径点为等价的, 然后取单位球面对于这个等价关系[I.2 §2.3] 的商[I.3 §3.3], [这个商就是实射影平面]. 定义实射影平面的第四个方法是从通常的欧几里得平面开始, 对于直线的每一个可能的"斜率", 即对每一族平行直线, 都附加上一个"无穷远点". 在适当的拓扑下, 这样就把实射影平面定义为欧几里得平面的一个紧化[III.9].

现在取第三个定义. 射影平面上的直线就定义为球面上的大圆 (但对径点算作同一点). 这时不难看到, 任意两条直线恰好交于一点 (因为任意两个大圆必定恰好交于一对对径点), 而任意两点必位于恰好一条直线上. 这个性质可以用来定义射影平面更抽象的推广.

对于 $\mathbf{R}$ 以外的其他的域和更高的维数, 也有类似的定义. 例如 n 维复射影空间, 就是所有形如 $(z_1,\cdots,z_n,z_{n+1})$ 的点的集合, 这里 z_i 是不全为 0 的复数, 而且规定对于所有不为 0 的复标量 λ, $(z_1,\cdots,z_n,z_{n+1})$ 和 $(\lambda z_1,\cdots,\lambda z_n,\lambda z_{n+1})$ 是等价的, 这也就是 $\mathbf{C}^{n+1}$ 中经过原点的直线的集合. 关于射影几何, 详见一些基本的数学定义[I.3 §6.7].

III.73 二 次 型
(Quadratic Forms)

Ben Green

一个二次型就是含有一组有限多个未知数 $x_1,x_2,\cdots,x_n$ 的二次齐次多项式, 一个例子是 $q(x_1,x_2,x_3)=x_1^2-3x_1x_2+4x_3^2$. 在这里系数 $1,-3,4$ 是整数, 但是这

个思想可以直截了当地从 $\mathbf{Z}$ 推广到任意的环 $\mathbf{R}$. 因为线性函数无可否认是重要的, 而 2 又是紧接着 1 的下一个正整数, 所以可以期望二次型也是很重要的, 事实上在许多不同的数学分支中, 包括线性代数, 也确实如此.

下面是两个关于二次型的定理.

定理 1 若 $\boldsymbol{x}, \boldsymbol{y}$ 和 $\boldsymbol{z}$ 是 $\mathbf{R}^d$ 中三个点, 则它们的距离满足下面的三角形不等式:

$$|\boldsymbol{x}-\boldsymbol{z}| \leqslant |\boldsymbol{x}-\boldsymbol{y}| + |\boldsymbol{y}-\boldsymbol{z}|.$$

定理 2 奇素数 p 可写成两个完全平方之和, 当且仅当它用 4 除的余数为 1.

说定理 1 与二次型有关, 这并不是一眼就可以看清的事情. 这样说的理由是欧几里得距离

$$|\boldsymbol{x}| = \sqrt{x_1^2 + \cdots + x_d^2}$$

的平方是实数域上的二次型 (这里 x_i 是 $\boldsymbol{x}$ 的分量). 这个二次型是从内积

$$\langle \boldsymbol{x}, \boldsymbol{y} \rangle = x_1 y_1 + \cdots + x_d y_d$$

中取 $\langle \boldsymbol{x}, \boldsymbol{x} \rangle = |\boldsymbol{x}|^2$ 而来的. 内积满足以下 4 个关系式:

(i) 对于所有的 $\boldsymbol{x} \in \mathbf{R}^d, \langle \boldsymbol{x}, \boldsymbol{x} \rangle \geqslant 0$, 而等号当且仅当 $\boldsymbol{x} = 0$ 时成立.

(ii) 对于所有的 $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z} \in \mathbf{R}^d$, $\langle \boldsymbol{x}, \boldsymbol{y}+\boldsymbol{z} \rangle = \langle \boldsymbol{x}, \boldsymbol{y} \rangle + \langle \boldsymbol{x}, \boldsymbol{z} \rangle$.

(iii) 对于所有 $\lambda \in \mathbf{R}$ 以及 $\boldsymbol{x}, \boldsymbol{y} \in \mathbf{R}^d$, 有 $\langle \lambda \boldsymbol{x}, \boldsymbol{y} \rangle = \lambda \langle \boldsymbol{x}, \boldsymbol{y} \rangle$.

(iv) 对于所有 $\boldsymbol{x}, \boldsymbol{y} \in \mathbf{R}^d$, $\langle \boldsymbol{x}, \boldsymbol{y} \rangle = \langle \boldsymbol{y}, \boldsymbol{x} \rangle$.

一般说来, 任意满足以上 4 个关系的函数 $\phi(\boldsymbol{x}, \boldsymbol{y})$ 都叫做内积. 三角形不等式就是可以论证为数学中最重要的不等式 ——*柯西–施瓦兹不等式*[V.19]

$$|\langle \boldsymbol{x}, \boldsymbol{y} \rangle| \leqslant |\boldsymbol{x}|\,|\boldsymbol{y}|.$$

$\mathbf{R}^d$ 上的所有二次型并非都是来自内积, 但是它们都是来自对称双线性形式 $\mathcal{G}: \mathbf{R}^d \times \mathbf{R}^d \to \mathbf{R}$. 所谓双线性形式就是一种两个变量的函数, 并且除了关于内积的上述公理 (i)(即所谓正性判据) 不一定满足以外, 满足内积的其余所有公理. 给定了一个二次型 $q(x)$ 以后, 就可以从下面的极化恒等式

$$\mathcal{G}(\boldsymbol{x}, \boldsymbol{y}) = \frac{1}{2}\left(q(x+y) - q(x) - q(y)\right)$$

来恢复一个双线性形式, 使得 $\mathcal{G}(\boldsymbol{x}, \boldsymbol{x}) = q(x)$. 当用其他的域 k 来取代 $\mathbf{R}$ 时, 二次型和对称的双线性形式的这种对应关系仍然成立(但是当 k 具有特征 2 时, 由于极化恒等式前有因子 $\frac{1}{2}$ 出现, 会产生严重的技术问题). 在线性代数中, 时常是先讨论

对称的双线性形式再来定义二次型. 这种抽象的途径比起本文开始时给的具体定义有一点好处, 就是这时不必指定 $\mathbf{R}^d$ 的基底.

如果基底的选择适当, 二次型的形状看起来会特别使人愉快, 可以这样来选择基底, 使得二次型成为下面的形式:

$$q(x) = x_1^2 + \cdots + x_s^2 - x_{s+1}^2 - \cdots - x_t^2,$$

这里 s 和 t 满足不等式 $0 \leqslant s \leqslant t \leqslant d$. $x_1, \cdots, x_t$ 就是 x 在特别选定的基底下的分量, 上式中正项的个数 s 与负项的个数 $t-s$ 之差 $s-(t-s)=2s-t$[①], 称为二次型的符号差 (signature). 当上式中只出现正项, 从而 $s=t=d$, 而负项不出现时, 这个二次型称为正定的 (定义欧几里得距离所用到的二次型就是这一类). 非正定的二次型也很常见, 例如, 二次型 $x^2+y^2+z^2-t^2$ 就被用来定义闵可夫斯基空间[I.3 §6.8], 它在特殊相对论中起关键的作用.

现在转到二次型在数论中的例子, 先从整数环 $\mathbf{Z}$ 上的两个著名定理开始. 第一个就是前面说的定理 2, 这是费马[VI.12] 发现的. 对于其他的二变量二次型如 x^2+2y^2 以及 x^2+3y^2 等等, 也有许多相关的结果. 然而, 一般的问题, 如哪些素数可以写为 x^2+ny^2, 却是极为细致有趣的问题, 而且引导到类域理论[V.28].

拉格朗日[VI.22] 在 1770 年证明了每一个数都可以写为 4 个完全平方之和. 事实上, 这种写法的个数 $r_4(n)$ 可以用下式来表示:

$$r_4(n) = \sum_{\substack{d \mid n \\ 4 \nmid d}} d.$$

这个公式可以用模形式[III.59] 理论来解释. 而模形式可以看作是数论中最重要的主题之一. 实际上, 它的生成级数

$$f(z) = \sum_{n=0}^{\infty} r_4(n) \mathrm{e}^{2\pi niz}$$

是一个 ϑ 级数, 由此, 它适合某些变换, 从而可以确认它是一个模形式.

康韦和 Schneeberger 有一个值得注意的定理指出, 如果一个二次型 $a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2$ (其中 $a_1, \cdots, a_4 \in \mathbf{N}$) 能够表示任意小于或等于 15 的正数, 则它能表示任意正数. 拉玛努金[VI.82] 列出了 55 个这样的二次型. 其实, 其中有一个不能表示 15, 但其余 54 个穷竭了所有这样的二次型. 例如每一个正数都可以写成 $x_1^2+2x_2^2+4x_3^2+13x_4^2$.

三个变量的二次型比较难处理. 高斯[VI.26] 证明了: 正整数 $n=x_1^2+x_2^2+x_3^2$ 当且仅当 n 不能写成 $4^t(8k+7)$ 这样的形状, 其中 t, k 是整数. 迄今尚未确切地知道哪些整数可以写成 $x_1^2+x_2^2+10x_3^2$(称为拉玛努金三元二次型) 的形式.

①原书误为 $s-t$. —— 中译本注

从素数理论的观点看来，一个变量的二次型最难理解. 例如，是否有无穷多个素数可以写成 x^2+1?

现在我们再来提一下最后一个主题，就是对于整数的未知数 $x_1, \cdots, x_n$，研究 $\mathbf{R}$ 上的二次型. 我们特别要提一下 Margulis 的一个漂亮的结果，证实了 Oppenheim 的一个猜想. 这个结果有一个如下的特例：对于任意的 $\varepsilon > 0$，可以找到整数 x_1, x_2 和 x_3 使得

$$0 < \left| x_1^2 + x_2^2\sqrt{2} - x_3^2\sqrt{3} \right| < \varepsilon.$$

证明使用了来自*遍历定理*[V.9] 的技巧，这个理论在自己的背景下是当今的研究中很有影响的前沿课题. 对于 x_1, x_2 和 x_3 的大小，迄今还没有得到显式的界限.

III.74　量 子 计 算 (Quantum Computation)

量子计算机是一个利用量子力学的"叠加现象"来进行计算的理论装置，它以一种基本上不同于经典方法的方式来进行计算，而在几种重要的情况下引人瞩目地更加有效. 在经典物理学中，对于某种性质，要么一个粒子可能具有这种性质，或者它没有这种性质. 但是按照量子力学，这个粒子却可能处于一种不确定的状况，即处于几个态的线性组合下，在其中有些态下，它具有这种性质，而在其中另外几个态下，它又没有这种性质. 这个线性组合的系数称为概率振幅 (probability amplitudes)，概率振幅就是与某个态相关的系数的模的平方，表示进行测量时发现粒子处于这个态的概率.

进行测量时究竟发生了什么事是使人困惑的，也是许多物理学家和哲学家正在热烈辩论的主题. 幸运的是，我们不必解决测量问题也能懂得量子计算 (现在大家就是这么称呼这种计算的). 其实，即使完全不懂量子力学也没有关系 (这有点像哪怕一个人完全不懂什么是晶体管，不知道它的工作原理，也可以在理论计算机科学上做出出色的工作，其理由是类似的).

为了懂得什么是量子计算，看一看计算的两个其他模型是有帮助的. 经典计算的概念是计算机里面实际进行的过程的数学提炼物. 计算机的"状态"，或简称为"态"，用一个 $n$bit 的串为其模型，这个串就是长度为 n 的 0 和 1 所成的序列. 用 σ 来表示一个典型的串，[也就是一个"态"]，而用 $\sigma_1, \sigma_2, \cdots, \sigma_n$ 表示构成这个态的各个 bit. "计算"就是一系列施加于初始的串 σ 上的非常简单的操作. 例如，下面就是一个可能的操作：选取任意三个数 i, j 和 k，它们都不大于 n. 对于当前的态 σ，如果 $\sigma_i = \sigma_j = 1$，就把 σ_k 变为 1，否则就变它为 0. 说这个操作为"简单"的，在于它是局部的，就是说，它对于 σ 的所作所为只依赖于也只影响到 σ 的有限多个 bit

(在现在的情况, 它只依赖于 σ_i 和 σ_j, 而只影响到 σ_k). 在这个模型里, 经典的计算机的 "态空间", 即所有可能的态的集合 Q_n, 就是所有长度为 n 的 0,1 序列的集合 $\{0,1\}^n$.

经过一定数目的阶段以后我们宣布计算已经完成. 这时, 再对终态进行一个简单的 "测量" 序列, 就是检查得到的串的各个 bit. 如果我们的问题是一个 "判定" 问题, 则典型地会这样来组织我们的计算, 使得最后只需要检查一个 bit: 如果它是 0, 则答案为 "否"; 如果它是 1, 则答案为 "是".

如果对上两段的思想还感到生疏, 我们强烈建议您在往下读之前, 先把条目计算复杂性[IV.20] 的前几节读一下.

我们要考虑的第二个模型是概率计算. 除了一点以外, 它和经典计算是一样的, 但在每一个阶段, 都允许我们投掷一次 (可能是偏心的) 硬币, 而我们进行的简单运算需视投掷的结果而定. 例如, 仍然取三个数 i, j 和 k, 但是下一步如下操作: 以 2/3 的概率进行原来的操作, 而以 1/3 的概率把 σ_k 换为 $1-\sigma_k$. 值得注意的是在算法中引入随机性将大有帮助 (同样值得注意的是从理论上说, 有很强的理由相信, 使用了随机性的算法都可以 "去随机化", 详见条目 [IV.20 §7.1]).

假设已经让随机化的概率计算进行了 k 步, 而我们还没有检验结果. 那么, 怎样建立计算机的当前态的模型呢? 可以使用经典计算同样的定义 —— 态就是一个 $n$bit 的串 —— 并且说我们的计算处于一个只有经过测量才能知道的态. 但是, 计算机的态并不是完全神秘不知的, 因为对于每一个 $n$bit 的串 σ, 都有一个态处于 σ 的概率 p_σ. 换言之, 把计算机的态看成 $Q_n = \{0, i\}^n$ 上的概率分布[III.71] 更好. 这个概率分布依赖于初始的态, 因此原则上提供了关于这个 $n$bit 的串的有用的信息.

下面说一下如何用随机计算来解决一个判定问题. 用 $P(\sigma)$ 来记以 σ 为初始的态而在计算结束时计算结果的某个 bit (不失一般性, 设为第一个 bit) 为 1 的概率. 假设可以这样来安排 P, 使得若判定问题的答案为 "是" 时, 对于一切 σ, $P(\sigma)$ 至少是 a; 而若判定问题的答案为 "否" 时, 对于一切 σ, $P(\sigma)$ 最多是一个较小的数 b. 取 a 和 b 的平均数 $c=\dfrac{1}{2}(a+b), b<c<a$. 现在把计算进行很多次, 次数为 m. 如果判定问题的答案为 "是", 则在计算结束时, 将有很高的概率使得 m 次计算中, 结果的第一个 bit 为 1 的次数超过 cm 次, 而若答案为 "否", 则第一个 bit 为 1 的次数将小于 cm 次. 这样, 对于判定问题的解答虽然不是完全确定的, 至少是产生错误的机会小得可以忽略不计.

概率计算机的 "态空间" 由 Q_n 上所有可能的概率分布构成, 换句话说就是由所有的函数 $p: Q_n \to [0,1]$ 构成, 但这个函数要适合条件 $\sum\limits_{\sigma\in Q_n} p(\sigma)=1$. 量子计算机的 "态空间" 也是由定义在 Q_n 上的函数构成的, 但是有两个重要的区别. 首先,

现在这些函数不但可以可取实值, 还可以取复值. 其次, 若 $\lambda : Q_n \to \mathbf{C}$ 是一个态, 则它需要适合的条件是 $\sum_{\sigma \in Q_n} |\lambda_\sigma|^2 = 1$. 换言之, λ 是希尔伯特空间[III.37] $l_2(Q_n, \mathbf{C})$ 中的单位向量, 而不是巴拿赫空间[III.62]$\ell_1(Q_n, \mathbf{R})$ 中的非负单位向量, 标量 λ_σ 就是前面提到的概率振幅. 这句话的意义在下面还要解释.

在量子计算机的可能的态中有所谓 "基底态"(basis state), 就是只在一个 $n$bit 的串上取值 1 而在其他 $n$bit 的串上取值 0 的态. 习惯上, 在此采用狄拉克的 "bra" $\langle|$(有人译为 "刁矢) 和 "ket"$|\rangle$(有人译为 "刃矢") 记号, 这样, 我们说的态 σ 就记为 $|\sigma\rangle$. 除了基底态以外的态称为 "纯态"(pure state), 就是基底态的线性组合, 这时, 仍然使用狄拉克记号. 例如当 $n = 5$ 时, $|\psi\rangle = \left(1/\sqrt{2}\right)|01101\rangle + \left(\mathrm{i}/\sqrt{2}\,|11001\rangle\right)$ 就是计算机的一个可能的态.

为了从一个态进到另一个态, 又需要施加一个 "局部的" 运算, 但是要把它改造得适合新的希尔伯特空间的背景. 先设有一个基底态 $|\sigma\rangle$. 又只看一个数目很小的 bit , 即只看三个数 i, j 和 k. 这时, 对于三元组 $\tau = (\sigma_1, \sigma_2, \sigma_3)$, [视每一个 σ_i 为 0 或 1, 有 8 个可能的态, 所以为了表示它们, 需要 8 个基底态. 在选择了相应的基底态以后], 就可以在一个小得多的态空间里来考虑它, 即在适合条件 $\sum_{\tau \in Q_3} |\mu_\tau|^2 = 1$ 的函数 $\mu : Q_3 \to [0, 1]$ 的空间里来考虑它. 在复希尔伯特空间里把一个单位向量映为一个单位向量的自然的运算是酉映射[III.50 §3.1], 我们所需要的确实也就是它们.

现在用一个例子来说明这些. 设 $n = 5$, 而 i, j 和 k 分别是 1, 3 和 4①. 在这三个 bit 上, 一个可能的运算是映 $|000\rangle$ 为 $\left(|000\rangle + \mathrm{i}\,|111\rangle\right)/\sqrt{2}$, 映 $|111\rangle$ 为 $(\mathrm{i}\,|000\rangle + |111\rangle)/\sqrt{2}$, 而让所有其他的 3 bit 序列不动. 如果我们开始的基底态是 $|01000\rangle$, [则其第 1, 3, 4 bit 是 0, 0, 0, 而第 2, 5 bit 是 1, 0. 所以, 若用所说的运算作用于它, 则令 2, 5 bit 不动, 保持为 1, 0, 另外的 1, 3, 4 bit 成为 $|000\rangle$, 则按上述的运算规则操作], 于是, 在操作结束时结果将是 $\left(|01000\rangle + \mathrm{i}\,|11110\rangle\right)/\sqrt{2}$.

现在我们已经解释了一个基本的运算对于基底态是怎样运行的, 事实上也就解释了对于一般的态是怎样做的, 因为基底态是态空间的基底. 换句话说, 如果从基底态的一个线性组合 (即叠加) 开始, 则可以按上面的方法作用于每一个基底态, 再对其结果作相应的线性组合即可.

这样, 量子计算的基本的运算就是用一种非常特别的酉映射作用于态空间上. 如果这个运算只是施加于 k 个 bit 上 (这个 k 实际上是很小的), 这个酉映射的矩阵将是对角形的分块矩阵: 在主对角线上有 2^{n-k} 个 $2^k \times 2^k$ 酉矩阵, 作用于这 k 个 bit 上 (基底的元素要适当排列). 一个量子计算就是一连串这种基本运算的序列.

测量量子计算的结果则比较神秘. 基本的思想是很简单的: 作了一连串基本运

①原书写的是 1, 2 和 4, 与下面的计算不符, 所以这里改动了.—— 中译本注

算后, 再来看作为结果的态的某一个 bit . 如果这个态不是一个基底态, 而是它们的线性组合, 这是什么意思呢? 答案是, 对于输出的序列的第 r 个 bit 进行 "量度" 就是在作一个概率过程, 但这个概率过程又与概率计算中的量度有些不同: 如果输出的态是 $\sum_{\sigma\in Q_n}\lambda_\sigma|\sigma\rangle$, 则我们测量到 1 的概率是所有 $|\lambda_\sigma|^2$ 对于这样的 σ 的和, 这些 σ 的第 k 个 bit 为 1; 而测量到 0 的概率则是上面的和对于第 k 个 bit 为 0 的 σ 来求和, 这就是 λ_σ 这些数称为概率振幅的原因. 为了从量子计算得出有用的结果, 需要把它重复进行多次. 在这一点上, 量子计算和概率计算是一样的.

请注意量子计算和概率计算的两个重要区别. 在概率计算中, 把概率计算的一个态描述为 Q_n 上的概率分布, 它是基底态的凸组合, [因为这个组合的系数都是非负实数]. 但是这个概率分布并没有告诉我们计算机里面是什么: 那是一个基底态. 这个概率分布对我们描述的是我们对于计算机里面的东西的一种知识. 但是, 量子计算机的态确实是一个 2^n 维希尔伯特空间的单位向量. 所以在一定意义下, 巨大的量的计算可以并行地进行, 量子计算的力量就在这里.

我们虽然对计算不可能知道太多, 因为一旦进行测量就会使得这个计算 "塌缩"(collapse), 我们却可以希望把计算组织起来, 使得它的各个部分互相 "干涉" (interfere). 这种干涉与量子计算和概率计算的第二个区别相关, 就是我们在量子计算中处理的是概率振幅, 而在概率计算中处理的是概率. 粗略地说, 量子计算可以 "分裂" 又 "重新组合", 而在概率计算中, 只要计算分裂了, 它就一直是分裂的. 对于量子计算中的重新组合, 至关重要的是概率振幅可以相消 (cancelation). 举一个极端的例子, 如果用酉矩阵的逆去乘这个酉矩阵, 这个过程中必然会有大量的相消, 才能使得在最终的结果中主对角线外的元素都变成 0.

以上所述提出了两个明显的问题: 量子计算机的好处在哪里? 以及是否真的能够造出量子计算机来? 量子计算机也能进行经典计算和概率计算, 所以第一个问题实际上问的是: 量子计算机还能不能做其他的事[①]. 我们可以这样想, 因为量子计算的态空间比经典计算的态空间大得无法比拟 (它是 2^n 维的, 而经典计算的态空间只是 n 维的), 而重组过程使我们能访问态空间的非常遥远的部分, 在那里, 系数可以是非常相似 (又非常小) 的, 然后又可以返回到原来的态, 并且作有用的测量. 然而, 态空间的极度广袤, 又使得绝大多数的态完全无法到达, 除非准备好了进行为数同样巨大的基本运算. 加之, 重要的是在计算结束时输出不应该是一个 "典型的" 态, 因为只有对于非常特别的态才能作有用的测量.

这些论据说明了一个量子计算机要想是有用的, 就必须要很小心地 (同时也很精巧地) 组织起来. 但是这种计算有一个奇观似的例子, 就是 Peter Shor 用量子计

①也可能经典地对量子计算作仿真, 但是真要这样做所需的时间大得离谱. 量子计算机不能计算不可计算函数, 但是计算某些可计算函数时, 它要有效得多.

算机极为快速地作了快速傅里叶变换[III.26]. 快速傅里叶变换的对称性使得我们可以把计算分裂开来 “并行地” 实现 (说是 “在叠加中” 计算更好). 这些使得它理想地适合于量子计算. 一个超快速傅里叶变换使得有可能 (用经典的方法) 解决一些著名的计算问题, 例如离散对数问题和大数的因子分解问题. 后者可以用于破解公钥密码系统, 这种加密方法是现代计算机安全的核心 (关于这些问题的进一步讨论, 可见条目数学与密码[VII.7 §5] 和计算数论[IV.3 §3]).

真能造出一个真正能做这些事情的计算机吗? 有极为艰巨的问题等待解决, 这些问题来自量子力学中的所谓 “退相干”(decoherence) 现象, 这个现象使得很难停止一个复杂态向较简单的无用的态 “塌缩”. 这方面取得了一些进展, 但是要说是否能够或者什么时候能够造出能够很快地分解大数为因子的量子计算机, 还为时过早.

尽管如此, 量子计算机的概念提出的理论上的挑战是非常诱人的. 这些挑战中最有趣的也是很简单的是找出一个量子计算机的应用, 使它与现在已经提出的少数几个应用有显著的不同. 量子计算机能够对大数作因子分解是它的巨大力量的强有力证据, 但是如果能更好地理解为什么如此就更好了 (现在已经知道, 量子计算机对于其他一些应用, 例如通信复杂性[IV.20 §5.1.4] 也比经典计算机更好). 是不是还有其他简单得多的任务, 对于经典计算机很难, 但是对于量子计算机很容易呢? 至少, 关于有些事情是计算机做不到的, 有一些似乎有道理的假设, 但是这些假设是真的吗? 量子计算机能解决 $\mathcal{NP}$ 完全性[IV.20 §4] 问题吗? 大多数人的意见是不行. 但是, 说它真的不能解决 $\mathcal{NP}$ 完全性问题, 这个命题现在也成了计算复杂性理论中的许多 “似然假设” 中的另外一个了. 想要人们相信这个新的似然假设还需要有更强的理由, 例如, 用量子计算来证明一个现在经典计算中还以似然假设为人所知的命题才行.

III.75 量子群 (Quantum Groups)

Shahn Majid

至少有三种不同的途径引向今天所称的量子群, 这些途径可以简明地概括成量子几何、量子对称和自对偶, 其中每一个都为量子群的发明提供了重大的理由, 也都在现代理论的发展中起了作用.

1. 量子几何

20 世纪物理学的重大发现之一是认识到经典力学应该为量子力学所取代. 在量子力学中, 提出了不可交换的位置和动量算子来代替经典力学中一个粒子的可能的位置和动量. 这种不可交换性构成了海森堡的 “不确定性原理” 的基础, 同时也

启发我们认识到：需要一种更广泛的几何概念，在其中坐标是不可交换的，在条目算子代数[IV.15 §5] 中讨论了处理非交换几何学的途径之一．但是还有另一个途径：注意到几何学实际上是从球面、环面等等例子中产生的，这些例子都是李群[III.48 §1] 或者是与李群有密切关系的对象．如果想把几何学量子化，就要考虑怎样把这些基本的例子加以推广，换句话说，就应该试着去定义“量子李群”以及相关的“量子齐性空间”．

不是用点而是用相应的代数来考察几何结构．例如群 $\mathrm{SL}_2(\mathbf{C})$ 定义为 2×2 的适合条件 $\alpha\delta-\beta\gamma=1$ 的复数矩阵 $\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$ 的集合，可以把它看作 $\mathbf{C}^4$ 的一个子集合，其实还不只是子集合，而是一个簇[III.95]．与这个簇相关的自然的函数类是限制在此簇上的 4 变量的多项式的集合 (这些多项式实际上是定义在整个 $\mathbf{C}^4$ 上的，但是，如果两个多项式在此簇上取同样的值，就视它们是等同的)．换句话说，取 4 变量 a,b,c 和 d 的多项式之集合，并对由 $ad-bc-1$ 生成的理想[III.81 §2] 取商[I.3 §3.3](这种构造方法将在条目算术几何[IV.5 §3.2] 中详细讨论)．把所得的代数记为 $\mathbf{C}[\mathrm{SL}_2]$．

对于任意由多项式关系定义的子集合 $X\subset\mathbf{C}^n$ 也能做这样的事，这就恰好给出了一个在这种类型的子集合与某个具有 n 个生成元的可交换代数之间的一一对应．用 $\mathbf{C}[X]$ 来记相应于 X 的代数，和许多类似的构造一样 (例如可见条目对偶性[III.19] 中关于伴映射的讨论)，一个由 X 到 Y 的映射，必生成一个由 $\mathbf{C}[Y]$ 到 $\mathbf{C}[X]$ 的映射．更确切地说，由 X 到 Y 的映射必须 (在一定意义下) 是多项式，而由 $\mathbf{C}[Y]$ 到 $\mathbf{C}[X]$ 的映射则是一个代数同态 ϕ^*，而且适合以下关系式：对所有的 $x\in X$ 和 $p\in\mathbf{C}[Y],\ \phi^*(p)(x)=p(\phi x)$．

回到我们的例子，集合 $\mathrm{SL}_2(\mathbf{C})$ 具有用矩阵乘法来定义的群结构：$\mathrm{SL}_2(\mathbf{C})\times\mathrm{SL}_2(\mathbf{C})\to\mathrm{SL}_2(\mathbf{C})$．$\mathrm{SL}_2(\mathbf{C})\times\mathrm{SL}_2(\mathbf{C})$ 又是 $\mathbf{C}^8$ 中的一个簇，矩阵的乘法则是按多项式方式依赖于矩阵的各个元素的，所以就会得到一个代数的同构 $\Delta:\mathbf{C}[\mathrm{SL}_2]\to\mathbf{C}[\mathrm{SL}_2]\otimes\mathbf{C}[\mathrm{SL}_2]$，称为上积 (coproduct)．($\mathbf{C}[\mathrm{SL}_2]\otimes\mathbf{C}[\mathrm{SL}_2]$ 同构于 $\mathbf{C}[\mathrm{SL}_2\times\mathrm{SL}_2]$)．结果，$\Delta$ 可以用下面的公式来表示：

$$\Delta\begin{pmatrix}a & b\\ c & d\end{pmatrix}=\begin{pmatrix}a & b\\ c & d\end{pmatrix}\otimes\begin{pmatrix}a & b\\ c & d\end{pmatrix}.$$

对这个公式需要解释几句话：a,b,c 和 d 是多项式代数 $\mathbf{C}[\mathrm{SL}_2]$ 的 4 个生成元 (就是多项式代数对于 $ad-bc-1$ 的商的 4 个生成元)，右方的乘积则是 $\Delta a=a\otimes a+b\otimes c$ 的简写，[这样的式子一共有 4 个]．所以 Δ 是定义在生成元上的某种张量积[III.89] 和矩阵乘积的混合物．

可以证明, SL_2 的矩阵乘法的结合性等价于 $(\Delta\otimes\mathrm{id})\,\Delta=(\mathrm{id}\otimes\Delta)\,\Delta$. 要想懂得这个式子的意义, 就要记住 Δ 是把 $\mathbf{C}\,[\mathrm{SL}_2]$ 的元映为 $\mathbf{C}\,[\mathrm{SL}_2]\otimes\mathbf{C}\,[\mathrm{SL}_2]$ 的元的. 这样, 例如当施行映射 $(\Delta\otimes\mathrm{id})\,\Delta$ 时, 先要施行 Δ 以得出一个 $\mathbf{C}\,[\mathrm{SL}_2]\otimes\mathbf{C}\,[\mathrm{SL}_2]$ 中的元 $p\otimes q$. 这个元是形如 $\Delta p\otimes q$ 的元的线性组合, 然后再把每一个 $p\otimes q$ 用 $\Delta p\otimes q$ 代替.

类似于此, $\mathrm{SL}_2\,(\mathbf{C})$ 的其他的群结构成分也都可以等价地用代数 $\mathbf{C}\,[\mathrm{SL}_2]$ 来表示, 例如其中的单位元现在对应于上单位映射 (counit map)$\in:\mathbf{C}\,[\mathrm{SL}_2]\to k$, 而群的逆元则相应于对径映射 (antipode map)$S:\mathbf{C}\,[\mathrm{SL}_2]\to\mathbf{C}\,[\mathrm{SL}_2]$. 群的公理就成了这些映射的相应的等价性质, 这样就使得 $\mathbf{C}\,[\mathrm{SL}_2]$ 成了一个 "霍普夫代数", 也就是一个 "量子群". 形式定义如下:

定义　域 k 上的霍普夫代数就是一个四元组 $(H,\Delta,\in,S)$ 使得

(i) H 是 k 上的一个具有单位元的代数 (unital algebra).

(ii) $\Delta:H\to H\otimes H,\in:H\to k$ 是代数的同态, 使得 $(\Delta\otimes\mathrm{id})\,\Delta=(\mathrm{id}\otimes\Delta)\,\Delta$, 以及 $(\in\otimes\mathrm{id})\Delta=(\mathrm{id}\otimes\in)\Delta=\mathrm{id}$.

(iii) $S:H\to H$ 是一个线性映射, 使得 $m\,(\mathrm{id}\otimes S)\,\Delta=m\,(S\otimes\mathrm{id})\,\Delta=1\in$, 这里 m 是 H 上的乘积运算.

关于这样的陈述, 有两件重要的事需要说明: 第一, 霍普夫代数的概念对于任意的域都是有意义的. 第二, 我们从没有要求 H 是可交换的. 当然, 如果 H 是从一个群导出的, 它自然是可交换的 (因为两个多项式的乘法可交换), 所以, 如果能够找到一个不可交换的霍普夫代数, 就找到了群概念的严格的推广. 过去 20 年的一大发现就是存在许多不可交换的例子.

例如量子群 $\mathbf{C}_q\,[\mathrm{SL}_2]$, 就定义为这样一个霍普夫代数: 它是符号 a,b,c 和 d 的自由的结合的不可交换代数, 而且 mod 了以下诸关系式:

$$\begin{gathered}ba=qab,\quad bc=cb,\quad ca=qac,\quad dc=qcd,\\ db=qbd,\quad da=ad+\left(q-q^{-1}\right)bc,\quad ad-q^{-1}bc=1,\end{gathered}$$

其中的 Δ 的定义和在 $\mathbf{C}\,[\mathrm{SL}_2]$ 中的 Δ 一样, 并有适当的 ε 和 S. 这里 $q\in\mathbf{C}$ 是其中的非 0 元, 而如果令 $q=1$, 就又得到 $\mathbf{C}\,[\mathrm{SL}_2]$. 这个例子可以对于所有的复单李群 G 推广为典则的例子 $\mathbf{C}_q\,[G]$.

群和李群理论的很大一部分都可以推广到量子群. 例如, 哈尔 (Haar) 积分就是一个对于平移不变的线性映射 $\int:H\to k$. 这里平移不变是在一定意义下说的, 而且涉及 Δ. 如果哈尔积分存在, 必定是在最多相差一个标量倍数意义下是唯一的. 而事实上, 在绝大多数有趣的情况, 包括所有的有限维霍普夫代数的情况, 它确实是存在的. 类似地, *微分形式*[III.16] 复形 (Ω,d) 在任意代数 H 上也是有意义的, 可

以用作为微分结构的代替物. 这里, $\Omega=\otimes_n\Omega^n$, 而由 $\Omega^0=H$ 和 Ω^1 生成, 但是我们并不像在经典情况下那样假设它是分级可交换的. 当 H 是一个霍普夫代数时, 我们要求 Ω 是平移不变的, 这在一定意义下又涉及上积 Δ. 这时, Ω 及其上同调[IV.6 §4], 作为复形, 都是超 (或分级) 量子群. 分级霍普夫代数的公理最早是由霍普夫在 1947 年引入的, 正是为了表示一个群的上同调环结构. 所以, 这个结果又转了一大圈回到了这个主题的起源. 对于绝大多数量子群, 包括所有 $\mathbf{C}_q[G]$, 都有一个最小的复形 (Ω,d). 这样, 一个 "量子群" 不单是一个霍普夫代数, 它还有附加的类似于李群的结构.

还存在许多其他的与 q 变形无关的量子群, 对于有限群理论也有应用. 设 G 是一个有限群, 就有一个定义在 G 上的函数所成的代数 $k(G)$, 其中有逐点乘积和上积 $(\Delta f)(g,h)=f(gh)$, 这里 $f\in k(G)$, $\quad g,h\in G$. 在此, 把 $k(G)\otimes k(G)$ 与 $k(G\times G)$ 等同起来, 这样就把 Δf 变成了一个二元函数. 验证它是一个霍普夫代数甚至还更加简单. 在一个有限集合上, 不会有有趣的经典的微分结构, 但是, 如果使用为量子群发展起来的方法, 则在任意有限群上也会有一个甚至多个平移不变复形 (Ω^1,d). 再应用微分几何量子群的其他部分, 还可以发现, 例如, 交错群 A_4 是自然地里奇 (Ricci) 平坦的, 而对称群 S_3 自然有常曲率[III.13], 很像 3 维球面.

2. 量子对称

在数学里, 对称时常是表现为一个群的作用或者某个结构的有限或无穷小变换的李代数的作用. 如果有一族变换, 而且此族变换在逆变换和复合下是封闭的, 就一定会有一个通常的群. 怎样推广这一点呢? 首先注意到, 一个群可以同时作用在几个对象上. 如果一个群作用在两个对象 X 和 Y 上, 那么它也就作用在其直积 $X\times Y$ 上, 如下式所示: $\Delta:G\to G\times G$, 它对左方的群 G 的每一个元素都作出其一个复本, 这样让这个元素作用在一个对象上, 而其复本则作用在另一个对象上. 为了推广这一点, 把群的概念代之以一个代数是值得的. 这一次使用群代数 kG. 它就是形式线性组合 $\sum\limits_i\lambda_iG_i$ 的集合, 这里 G_i 是群 G 的元素, 而 λ_i 则是域 k 中的标量. G 的元素 (看作是最简单的线性组合) 构成 kG 的基底, 而其乘法就是群 G 中的乘法, 然后就把这样的乘法以明显的方式推广为一般的线性组合的乘积. 也把 Δ 从对于基底元素 G 的 $\Delta G=G\otimes G$ 推广到从 kG 到 $kG\otimes kG$ 的映射. 再加上两个附加的映射 $\in$ 和 S, 就使得 kG 变成了一个霍普夫代数. 注意, 上积在这里的使用方法与在上一节中的使用方法完全不同, 因为现在群的乘积已经进入代数了. 对于与任意李代数 g 相关的 "包络代数"(enveloping algebra)$U(g)$ 也有类似的一番道理, 它是由 g 的带有若干关系的基底生成的, 并且变成了一个霍普夫代数, 其中的上积 $\Delta\xi=\xi\otimes1+1\otimes\xi$ 把 g 中的元素 ξ"分拆" 开来, 以便作用于 g 所作用的对象的张量积上.

从这两个例子外推, 一个一般的 "量子对称" 意味着一个代数 H 赋有一个进

一步的结构 Δ, 使得对于 g 的任意两个表示 V 和 W 都能够构造出服从结合律的张量积 $V \otimes W$. H 的任意元素 h 都按照 $h(v \otimes w) = (\Delta h)(v \otimes w)$ 来作用, 即 h 的一部分作用在 $v \in V$ 上, 另一部分则作用在 $w \in W$ 上. 这就是在前一节里讲的霍普夫代数的公理的第二条途径.

注意, 在上面的例子里面, Δ 的输出已经是对称的. 因此, 如果 V 和 W 是一个群的表示或者一个李代数的表示, 则 $V \otimes W$ 和 $W \otimes V$ 通过一个明显的映射 $v \otimes w \to w \otimes v$ 而互相同构. 但是, 一般说来, $V \otimes W$ 和 $W \otimes V$ 是没有关系的, 所以现在是张量积被做成不可交换的. 在好的情况下, $V \otimes W \cong W \otimes V$, 但是不一定是通过上面说的那个明显的映射. 事实上, 对于每一对 V 和 W, 只要服从某些合理的条件, 就都可能有非平凡的同构. 对于很大一类例子, 记作 $U_q(\mathrm{g})$, 会出现这样的情况, 这类例子与所有的复单李代数相关. 对于这些例子, 上述的同构服从三个表示的辫关系, 即 Baxter-Young 关系 (见条目*辫群*[III.4]). 因此, 这些量子群引导到扭结和 3 *维流形不变量*[III.44](琼斯扭结不变量就来自 $U_q(\mathrm{sl}_2)$, sl_2 是群 $\mathrm{SL}_2(\mathbf{C})$ 的李代数. 在此把参数 q 看作一个形式变量是很有用的, 而这些例子都可以看作是经典的包络代数 $U(\mathrm{g})$ 的某种变形, 它们来自 Drinfeld 和 Jimbo 关于量子可积系统的工作.

3. 自对偶

第三个观点是霍普夫代数是简单性仅次于阿贝尔群而又允许*傅里叶变换*[III.27]的*范畴*[III.8]. 这一点并不是马上就明显可见的, 但是, 前面给出的霍普夫代数的公理 (i) 到 (iii) 具有某种对称性. 可以把具有单位元的代数 H 的公理 (i) 用线性映射 $m: H \otimes H \to k,\quad \eta: k \to H$ 来表示 (这里 η 可用以确定 H 单位元作为 $1 \in k$ 的像), 而这种表示要服从一些可交换图式. 如果把这些图式中的箭头都反转过来, 就会得到公理 (ii), 而得出的东西可以称为一个 "上代数"(coalgebra). 要求上代数结构 Δ 和 $\in$ 也是代数映射, 就给出一族在箭头反转时也不变的可交换图式. 最后, 公理 (iii) 作为可交换图式, 在上述意义下在箭头反转时也是不变的.

这样, 霍普夫代数的公理有一个特别的性质, 就是它们在箭头反转时是对称的. 一个实际的推论是, 若 H 是一个有限维霍普夫代数, 则 H^* 也是, 而且其所有的结构映射都可以定义为 H 的相应结构的伴 (这就自然把箭头方向反转). 在无限维情况, 就需要一个适当的拓扑对偶, 这样就可以说这两个霍普夫代数互为对偶配对的. 例如 $\mathbf{C}_q[\mathrm{SL}_2]$ 和 $U_q(\mathrm{sl}_2)$ 就是对偶配对的, 而若 G 是有限群, 则 $(kG)^* = kG$ 就是 G 上的函数所成的霍普夫代数.

作为一个应用, 令 H 是有限维的而有基底 $\{e_a\}$, 令 H^* 有对偶基底 $\{f^a\}$, 而 $\int$ 是 H 上的右平移不变积分. 于是, 傅里叶变换 $F: H \to H^*$ 就定义为

$$F(h) = \sum_a \left(\int e_a h\right) f^a.$$

它有许多值得注意的性质. 一个特例是对于有限不一定是阿贝尔群的 G 的傅里叶变换 $F: k(G) \to kG$, 如果 G 是阿贝尔群, 则 $kG \cong k\left(\hat{G}\right)$, $\hat{G}$ 是特征标群, 这样就回到了有限阿贝尔群的通常的傅里叶变换. 要点在于在非阿贝尔情况, kG 是不可交换的, 因此不是通常的"傅里叶对偶"空间上的函数的代数.

第二个主要类别的真正量子群的发现, 主要就是由于这个观点. 这一类量子群就是所谓自对偶"双叉积"(bicrossproduct) 量子群. 它们同时是"坐标"代数, 也是"对称性"代数, 而且与量子力学确实有关. 有一个例子, 通常写为

$$\mathbf{C}[\mathbf{R}^3 >\!\!\triangleleft \mathbf{R}]\lambda \blacktriangleright\!\!\triangleleft U(\mathrm{so}(1,3)),$$

就是坐标为 x, y, z, t 的某个不可交换时空 (t 与其他变量不可交换) 的庞加莱量子群. 这个量子群可以解释为在具有黑洞特点的弯曲空间中运动粒子的量子化. 从本质上说, 量子群的自对偶性给出了引力 (作为时空的几何) 和量子理论统一的"玩具模型"的一个范式.

量子群只是一个更大的背景的一部分. 图 1 上画出了这个背景的图示[①]. 对象的一个范畴, 如果具有相容的"张量积"概念, 就称为是一个单项范畴 (monoidal category) (或张量范畴 (tensor category)), 我们已经看到, 量子群的表示就是一个单项范畴. 在那里还有一个"遗忘函子"(forgetful functor), 把它映到向量空间范畴, 而忘记量子群的作用. 这就把量子群嵌入到下一个 (在表示论意义下的) 最一般的自

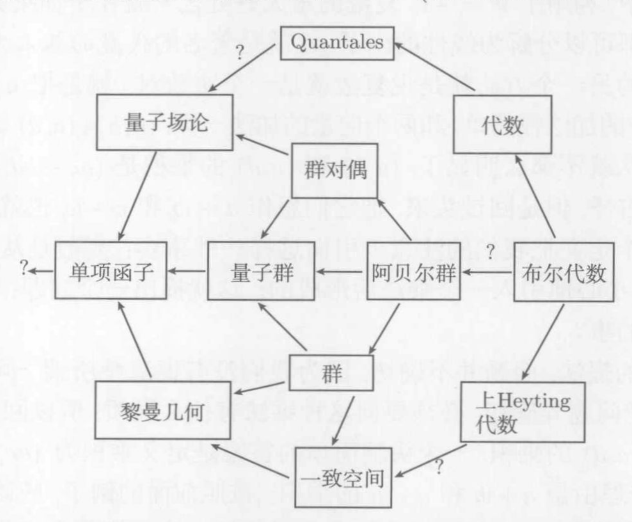


图 1 把量子群放到它的背景中, 水平轴上画的是自对偶范畴

①图 1 顶端有一个方框, 注明是一个 quantales. 但是正文没有提到这个概念, 译者也没有找到合适的中文译文, 所以只能照录于此. 粗略地说, 它是一个相当广泛而又抽象的代数结构. 有兴趣的读者可以在下面的网址找到初步的介绍: http://en.wikipedia.org/wiki/Quantale.—— 中译本注

对偶范畴, 即成为单项范畴之间的函子. 在此图的最右方, 放进了布尔代数, 作为一个具有德 · 摩根对偶的原始的结构. 然而, 这里的对偶性和其他的对偶性的联系, 还只是思辨性质的.

进一步阅读的文献

Majid S. 2002. *A Quantum Group Primer*. London Mathematical Society Lecture Notes, volume 292. Cambridge: Cambridge University Press.

III.76 四元数, 八元数和赋范除法代数 (Quaternions, Octonions, and Normed Division Algebras)

随着复数[I.3 §1.5] 的引入, 数学在深奥和微妙上走了一大步. 为了定义复数, 先得把对于虚数和复数的不信任感放在一旁, 引入一个新数 i, 直接宣布 $\mathrm{i}^2 = -1$. 一个典型的复数的形状是 $a + \mathrm{i}b$, 而复数的算术可以从通常的实数算术得出. 例如, 要计算 $1 + 2\mathrm{i}$ 和 $2 + \mathrm{i}$ 的乘积, 只要把括号展开就行了:

$$(1 + 2\mathrm{i})(2 + \mathrm{i}) = 2 + 5\mathrm{i} + 2\mathrm{i}^2 = 5\mathrm{i}.$$

最后一步中, 利用了 $\mathrm{i}^2 = -1$. 复数的重大好处之一就在于如果允许了复根, 每一个多项式就都可以分解为线性的因子, 这就是著名的代数的基本定理[V.13].

定义复数的另一个方法就是说复数就是一个实数对, 就是把 $a + \mathrm{i}b$ 直接写成 (a, b). 两个复数的加法很简单, 和两个向量的加法一样: $(a, b)+(c, d) = (a + c, b + d)$. 但是怎样做乘法就不那么明显了, (a, b) 和 (c, d) 的乘积是 $(ac - bd, ad + bc)$. 这个定义看起来很古怪, 但是回过头来, 把它们想作 $a + \mathrm{i}b$ 和 $c + \mathrm{i}d$ 也就清楚了.

但是第二个定义把我们的注意力引向这样一件事实: 复数是从 2 维向量空间[I.3 §2.3]$\mathbf{R}^2$ 中小心地引入一个乘法后形成的. 这就提出一个问题: 对于高维空间能不能做同样的事?

按照这样的提法, 问题并不确切, 因为我们没有说清楚所谓"同样的事"是什么意思. 为了把问题弄确切, 必须要问这种乘法有什么性质, 所以回到 $\mathbf{R}^2$. 对于什么是 (a, b) 和 (c, d) 的乘积, 一个头脑简单的答案是定义乘积为 (ac, bd). 这当然是不行的, 其部分理由是 $a+\mathrm{i}b$ 和 $c+\mathrm{i}d$ 的乘积, [按照前面的例子, 应该是 $(ac - bd) + \mathrm{i}(ad + bc)$], 而不能是 $ac + \mathrm{i}bd$. 但是能不能用其他方法来把两个 $\mathbf{R}^2$ 向量相乘呢?

上面提出的那种乘法的"头脑简单"的定义, 还有一个麻烦在于它允许有零因子出现, 即有一对非零的数, 乘起来以后会给出零. 例如, 按这个公式会有 $(1, 0)(0, 1) = (0, 0)$. 如果有零因子, 就不会有乘法逆, 因为在一个数域中, 每一个非零的数都有

乘法逆, 而如果 $xy=0$, 则要么 $x=0$, 要么 $y=x^{-1}xy=x^{-1}0=0$. 如果没有乘法逆, 就不能定义有用的除法概念.

现在回到复数的通常的定义, 并且仔细想一想怎样才能超越复数. 如过去那样做 "同样的事" 的一个方法是: 对复数做曾经对实数做过的事情. 就是说, 何不定义 "超复数" 就是一个有序的复数对 (z,w)? 因为我们还想得到一个向量空间, 就会仍然定义 (z,w) 和 (u,v) 的和为 $(z+u,v+w)$, 但是, 我们还必须想一下定义它们的乘积的最好的办法. 一个显而易见的猜想就是继续用前面对于通常的复数管用的表达式, 而定义它们的乘积为 $(zu-wv,zv+wu)$. 但是如果这样做, 则把 $(1,\mathrm{i})$ 和 $(1,-\mathrm{i})$ 的乘积算出来, 就是 $(1+\mathrm{i}^2,\mathrm{i}-\mathrm{i})=(0,0)$, 所以又有了零因子.

这个例子来自以下的思想, 复数 $a+\mathrm{i}b$ 的模, 即实数 $|z|=\sqrt{a^2+b^2}$, 是量度向量 (a,b) 的长度的, 它也可以写为 $\sqrt{\bar{z}z}$, 这里 $\bar{z}$ 就是 z 的共轭复数 $a-\mathrm{i}b$. [这里 a 和 b 都是实数], 如果允许 a 和 b 取复值, 则 a^2+b^2 没有理由仍然保持为非负实数, 所以也就没有办法使它的平方根仍为实数. 此外, 如果 $a^2+b^2=0$, 得不出 $a=b=0$. 上面的例子就来自利用这里的想法, 令 $a=1,b=\mathrm{i}$, 而且用 $(a,b)=(1,\mathrm{i})$ 的 "共轭"$(1,-\mathrm{i})$ 去乘它而得到的.

然而, 有一个自然的方法来定义数对 (z,w) 的模, 使得即令 z 和 w 都是复数时仍然可用. 数 $|z|^2+|w|^2$ 保证是非负的, 所以可以取它的平方根. 如果 $z=a+\mathrm{i}b, w=c+\mathrm{i}d$, 则将得到模为 $\left(a^2+b^2+c^2+d^2\right)^{1/2}$, 它就是向量 (a,b,c,d) 的长度.

这一件事实引导到另外一个观察: 实数的复共轭就是它自身, 那么, 如果想对复数也如对实数做 "同样的事", 就能自由地把复共轭引入我们的公式. 在试着去这样做以前, 先想一下数对 (z,w) 的共轭可能意味什么. 我们希望 $(z,0)$ 的性态如 z 一样, 所以它的共轭应该是 $(\bar{z},0)$. 类似地, 如果 z,w 都是实数, 则 (z,w) 的共轭应该是 $(z,-w)$. 这样, 对于一般的数对 (z,w) 余下只有两个可能性: 它的共轭或者是 $(\bar{z},-\bar{w})$, 或者是 $(\bar{z},-w)$. 我们来考虑第二种情况. [以后, 我们确实是以 $(\bar{z},-w)$ 作为 (z,w) 的共轭的定义的].

我们希望 (z,w) 与其共轭 (现在定义为 $(\bar{z},-w)$) 的乘积是 $(|z|^2+|w|^2,0)$, 希望这样就可以通过把复共轭引入通常的复数的乘积公式

$$(z,w)(u,v)=(zv-wu,zu+wv),$$

这样来得出我们所希望的结果. 一个明显的方法是令乘积公式为

$$(z,w)(u,v)=(zu-\bar{w}v,\bar{z}v+wu),$$

[这也就是实际采用的复数对的乘积的定义], 这样就会得到复数对 (z,w) 的集合上的一个结合的*二元运算*[I.2 §2.4]. 如果采用定义共轭的第一种可能性, 就会得到零因子 (这个麻烦的最初表现就是数对 $(0,\mathrm{i})$ 的共轭是它自身).

我们刚才定义的数对叫做一个四元数, 记这些"数"的集合为 $\mathbf{H}$, 则 $\mathbf{H}$ 是一个 4 维的实向量空间 (字母 $\mathbf{H}$ 是为了纪念四元数的发现者哈密顿 (William Rowan Hamilton), 见条目哈密顿[VI.37]). 但是为什么我们希望这样做呢? 何况这样定义的乘法是不可交换的, 例如, $(0,1)(\mathrm{i},0)=(0,\mathrm{i})$, 而 $(\mathrm{i},0)(0,1)=(0,-1)$. 一旦发现这一点, 回答为什么要这样做这个问题就更迫切了.

为了回答这个问题, 我们退回来再想一想复数. 引入复数最明显的依据就是可以用复数来解出所有的多项式, 但这绝非唯一的依据. 特别是复数有重要的几何解释, 即解释为旋转加上拉伸. 如果对 $a+ib$ 再引入矩阵记号 $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$, 它与几何的联系就更加清楚了. 乘以复数 $a+ib$ 可以看成是平面 $\mathbf{R}^2$ 上的一个线性变换, 而上面的矩阵就是这个线性变换的矩阵, 例如复数 i 对应于矩阵 $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, 而这恰好就是绕原点逆时针方法旋转 $\dfrac{\pi}{2}$, 而乘以 i 也就是在复平面上作这个旋转.

如果说复数可以看成 $\mathbf{R}^2$ 到 $\mathbf{R}^2$ 的线性映射, 则四元数可以看成 $\mathbf{C}^2$ 到 $\mathbf{C}^2$ 的线性映射, 而我们就是这样看的. 现在把复数对 (z,w) 与矩阵 $\begin{pmatrix} z & \bar{w} \\ -w & \bar{z} \end{pmatrix}$ 联系起来, 考虑两个这类矩阵的乘积公式

$$\begin{pmatrix} z & \bar{w} \\ -w & \bar{z} \end{pmatrix}\begin{pmatrix} u & \bar{v} \\ -v & \bar{u} \end{pmatrix}=\begin{pmatrix} zu-\bar{w}v & z\bar{v}+\bar{w}\bar{u} \\ -\bar{z}v-wu & \bar{z}\bar{u}-w\bar{v} \end{pmatrix}.$$

这个矩阵恰好就是与复数对 $(zu-w\bar{v}, zv+w\bar{u})$ 相联系的矩阵, 而这个复数对, 作为四元数, 恰好是在上面给出的数对 (也就是四元数)(z,w) 与 (u,v) 的乘积! 作为一个直接的推论, 即有四元数的乘法是结合的. 为什么? 因为矩阵乘法是结合的 (而后者之所以是结合的, 又因为映射的复合是结合的, 见 [I.3 §3.2]).

注意, 矩阵 $\begin{pmatrix} z & \bar{w} \\ -w & \bar{z} \end{pmatrix}$ 的行列式[III.15] 等于 $|z|^2+|w|^2$, 所以数对 (z,w) 的模 (其定义为 $\sqrt{|z|^2+|w|^2}$) 就是相应的矩阵的行列式, 这就证明了两个四元数乘积的模等于其模的乘积 (因为乘积的行列式等于行列式的乘积). [因此, 四元数的乘法没有零因子]. 还要注意, 这个矩阵的伴 (即转置矩阵的共轭) 是 $\begin{pmatrix} \bar{z} & -\bar{w} \\ w & z \end{pmatrix}$, 它也就是与数对的共轭 $(\bar{z},-w)$ 相应的矩阵. 最后还要注意, 如果 $|z|^2+|w|^2=1$, 则

$$\begin{pmatrix} z & \bar{w} \\ -w & \bar{z} \end{pmatrix}\begin{pmatrix} \bar{z} & -\bar{w} \\ w & z \end{pmatrix}=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

这就告诉了我们, 相应于四元数 (z,w) 的矩阵 $\begin{pmatrix} z & \bar{w} \\ -w & \bar{z} \end{pmatrix}$ 是一个酉矩阵. 反过来, 也容易证明, 行列式为 1 的 2×2 酉矩阵一定可以写为 $\begin{pmatrix} z & \bar{w} \\ -w & \bar{z} \end{pmatrix}$ 的形式. 所以, 单位四元数 (即模为 1 的四元数) 有一个几何解释: 它们相应于 $\mathbf{C}^2$ 的 "旋转"(即行列式为 1 的酉映射), 正如单位复数相应于 $\mathbf{R}^2$ 上的旋转一样.

$\mathbf{C}^2$ 上的行列式为 1 的酉映射构成一个重要的*李群*[III.48 §1], 称为特殊酉群, 记号是 SU(2). 另一个重要的李群是 SO(3), 即 $\mathbf{R}^3$ 中的旋转的群. 令人吃惊的是, 单位四元数也可以用于描述这个群. 为了看到这一点, 把四元数用另一个更加传统的方法来表示是很方便的.

四元数传统上是这样引入的, 它是这样一个数系, 其中 -1 并不是只有 1 个独立的平方根, 而是有 3 个独立的平方根, 分别记为 i, j 和 k. [它们服从以下的关系式: $\mathrm{i}^2=\mathrm{j}^2=\mathrm{k}^2=-1$, 以及 $\mathrm{ij}=\mathrm{k},\mathrm{jk}=\mathrm{i},\mathrm{ki}=\mathrm{j}$]. 只要知道了这些关系式, 就得到了作四元数的乘法所需要的全部信息. 例如, 容易证明 $\mathrm{ji}=\mathrm{jjk}=-\mathrm{k}$. 一个典型的四元数可以写成 $a+\mathrm{i}b+\mathrm{j}c+\mathrm{k}d$, 它对应于复数对 $(a+\mathrm{i}c,b+\mathrm{i}d)$, 而这就是前面把四元数看成复数对的想法. 但是现在也可以把四元数看成这样一个对子 (a,v), 这里 a 是一个实数, 而 $v=(b,c,d)$ 是一个 $\mathbf{R}^3$ 向量. 现在把两个四元数 (a,v) 和 (b,w) 的乘积按以前给出的公式算出来, 就会得到 $(ab-v\cdot w, aw+bv+v\wedge w)$, 其中 $v.w$ 和 $v\wedge w$ 分别是 v 和 w 的数量积和向量积.

如果 $q=(a,u)$ 是一个模为 1 的四元数, 则 $a^2+\|u\|^2=1$, 所以可以把 q 写成 $(\cos\theta, v\sin\theta)$ 的形式, 其中, a 是一个实数, 而 v 是 $\mathbf{R}^3$ 中的一个单位向量. 四元数相应于 $\mathbf{R}^3$ 中的一个旋转 R, 旋转轴的方向就是向量 v, 而旋转角则是 2θ, 这里的旋转角和上面说的 "相应" 的方式, 都不是如我们一开始想象的那个样子. 如果 w 是另外一个 $\mathbf{R}^3$ 向量, [那么, 对它作上面说的旋转 R, 则 Rw 是什么样子呢? 下面就来回答这个问题]. w 可以用四元数表示为 $(0,w)$, 现在要给四元数 $(0,Rw)$ 一个干净利落的表达式, 我们的结果是 $(0,Rw)=q\cdot(0,w)\cdot q^*$, 这里的 q 就是前面说的 $(\cos\theta, v\sin\theta)$, q^* 则是它的共轭 $(\cos\theta,-v\sin\theta)$, 因为 q 的模是 1, 所以现在 q^* 也是 q 的乘法逆: $q^*=q^{-1}$. 这就是说, [为了作 3 维旋转 R, 和 2 维旋转不同, 现在不是像 2 维情况那样, 用一个单位复数去作乘法, 而是用一个单位四元数 q 去作 "共轭运算"]. 这里所谓 "共轭运算" 并不是例如求共轭复数, 甚至不是求共轭四元数的那种共轭, 而是在群的意义下 (见 [I.3 §3.3]) 左乘以 q, 再右乘以 $q^{-1}=q^*$ 的那种 "共轭". 现在, 若 q_1,q_2 是相应于旋转 R_1,R_2 的四元数, 则

$$q_2q_1\cdot(0,w)\,q_1^*q_2^*=(q_2q_1)\cdot(0,w)\cdot(q_2q_1)^*,$$

由此可知 q_2q_1 相应于旋转 R_2R_1, 这说明四元数的乘法相应于旋转的复合.

单位四元数构成一个群. 我们已经指出, 这个群就是 SU(2). 看来可能 SU(2) 就是 SO(3), 但是这一点并未得到完全的证明, 因为 $\mathbf{R}^3$ 的每一个旋转都有两个单位四元数会产生它. 理由很简单: 绕某个向量 v 按逆时针方向旋转一个角 θ 和绕 $-v$ 按逆时针方向旋转 $-\theta$ 是同一回事. 换言之, 如果 q 是一个单位四元数, 则 q 和 $-q$ 生成 $\mathbf{R}^3$ 的同一个旋转. 所以, SU(2) 并不同构于 SO(3), 而宁可说是 SO(3) 的双重覆盖. 这件事在数学和物理学中有重要的含义, 特别是它可以解释基本粒子的 "自旋" 概念.

现在回到以前提出的一个问题: 对于哪些 n, 能够找到 $\mathbf{R}^n$ 中向量的乘法的好的定义? 我们已经知道, 对于 $n=1,2$ 和 4 都可以. 但是在 $n=4$ 时, 要牺牲可交换性, 但是我们为此得到了丰厚的回报, 因为四元数乘法是表示重要的李群 SU(2) 和 SO(3) 的简明的方法. 这些群都是不可交换的, 所以对于我们能够取得成功至为本质的一点, 是未曾要求四元数的乘法为可交换的.

一个可能的做法是继续前面导致四元数的方法. 所以, 可以把一个四元数对 (q,r)[作为新的 "数" 的定义], 而用下面的式子, 规定其乘法为

$$(q,r)(s,t)=(qs-r^*t,q^*t+rs).$$

因为四元数 q 的共轭 q^* 正是复数 z 的复共轭 $\bar{z}$ 的类比, 此式基本上就是复数对 —— 即四元数 —— 乘法的公式.

然而, 我们要小心了, 四元数的乘法是不可交换的, 所以可以写出许多和上面这一个 "基本上是一样的" 公式. 那么为什么选用上面这一个, 而不把例如其中的 q^*t 换成 tq^* 呢?

可以证明, 我们在上面建议的式子允许有零因子存在. 例如, 把 $(\mathrm{i},\mathrm{j})(1,\mathrm{k})$ 按上面的公式算出来, 就会得到 $(0,0)$. 然而, 如果把这个公式修改为

$$(q,r)(s,t)=(qs-tr^*,q^*t+sr),$$

则只要记住我们希望 $(q,r)(q^*,-r)$ 会给出 $(|q|^2+|r|^2,0)$, 那么很快就会发现这个公式可以生成一个有用的数系. 这个数系我们记作 $\mathbf{O}$, 而其元素则称为八元数 (octonions)(有时也称为凯莱 (Cayley) 数). 不幸的是, 八元数的乘法甚至是非结合的, 但是它们确有两个很好的性质: 其一, 每一个非零的八元数都有乘法逆; 其二, 两个非零的八元数相乘绝不会给出零 (因为八元数的乘法是非结合的, 这两个性质不再 [如四元数那样] 是显然等价的, 但是八元数系的任意由两个元素生成的子代数却是结合的, 所以在那里, 这就足以证明其等价性).

这样, 当维数是 1, 2, 4 或者 8 时, 是可以做出所需要的数系的. 可以证明, 这些是仅有的具有很好的乘法概念的维数. 当然, 所谓 "好" 是有技术的含义的, 例如矩阵的乘法, 虽然有零因子, 但是是结合的. 如果只就这一点而言, 它就比八元数乘

法的定义 "更好", 后者没有零因子, 但是也没有结合律. 所以, 余下的就是要看一看, 1, 2, 4 和 8 这些维数有什么特别的地方.

所有上面构造出来的数系都有由*范数*[III.62] 所定义的大小. 对于实数和复数 z, 范数就是它的模. 对于四元数或八元数 x, 范数就是 $\sqrt{x^*x}$, 这里 x^* 是 x 的共轭 (这个说法, 对于实数和复数也可以用). 如果用 $\|x\|$ 表示 x 的范数, 则说明我们所定义的范数都具有以下的性质: 对于一切 x 和 y, 都有 $\|xy\| = \|x\|\|y\|$. 这个性质是极为有用的, 例如它告诉我们, 范数为 1 的元素的集合在乘法下是闭合的. 这个性质, 在讨论复数和四元数的几何的重要性时已经用过多次.

使得维数 1, 2, 4 和 8 区别于其他维数的特性, 就在于它们是仅有的使得我们能够定义一个具有以下的性质范数和乘法概念的维数. 这些特性如下:

(i) 有乘法恒等元 1, 使得对于所有的元素 x 都有 $1 \cdot x = x \cdot 1 = x$.

(ii) 乘法是双线性的, 意思上对于每一个 x, y 和 z 都有 $x(y+z) = xz + yz$, 以及 $(x+y)z = xz + yz$; 而且当 a 为实数时, $(ax)y = x(ay) = a(xy)$①.

(iii) 对于任意的 x 和 y, 都有 $\|xy\| = \|x\|\|y\|$(因此没有非零的零因子).

一个赋范除法代数, 就是一个向量空间 $\mathbf{R}^n$, 其中有范数的概念, 向量之间又有乘法, 而范数和乘法具有上面的三条性质. 只有当 $n = 1, 2, 4$ 和 8 时, $\mathbf{R}^n$ 才是赋范除法代数. 进一步, 在这些维数下面, 仅有的赋范除法代数的例子就是 $\mathbf{R}$(实数)、$\mathbf{C}$(复数)、$\mathbf{H}$(四元数) 和 $\mathbf{O}$(八元数).

这个事实称为赫尔维茨 (Hurwitz) 定理 ②, 它有许多证法. 下面是证法之一的简明描述. 证法的思想是去证明如果一个赋范除法代数 A 包含了上面四个例子之一, 则要么它就是这个例子, 要么它还包含了这个序列中的下一个. 所以, 要么 A 就是 $\mathbf{R}, \mathbf{C}, \mathbf{H}$ 或 $\mathbf{O}$, 要么 A 还包含了由对于 $\mathbf{O}$ 施行由 $\mathbf{C}$ 构造 $\mathbf{H}$、由 $\mathbf{H}$ 构造 $\mathbf{O}$ 的过程所得的结构, 这个过程称为凯莱–迪克森 (Cayley-Dickson) 构造. 然而, 对 $\mathbf{O}$ 施加凯莱–迪克森构造, 将会得到一个含零因子的代数.

想要看一看这个论证是怎样进行的, 可以设 A 包含了 $\mathbf{O}$ 为其真子代数. 可以证明, A 上的范数一定就是*欧几里得范数*[III.37], 即由内积得出的范数 (粗略地说, 用一个范数为 1 的元素去乘, 不会改变范数, 这就使得 A 具有许多对称性, 所以 A 上的范数应该是最为对称的范数, 这就是欧几里得范数). 把 A 中正交于 1 的元素称为虚元素, 然后就可以在 A 上定义共轭算子如下: 定义 $1^* = 1$, 而若 x 是虚元素, 就定义 $x^* = -x$, 以下再按照线性关系来拓展这个定义. 可以证明, 这个算子具有所有我们希望它具备的性质. 特别是对于 A 中的任意元素 a 都有 $a^*a = aa^* = \|a\|^2$.

---

①原书 (ii) 不甚恰当. 因为现在的乘法是非交换的, 所以给了 $x(y+z) = xy+xz$ 后得不出 $(x+y)z = xz + yz$. 这里作了改正.—— 中译本注

②数学中有许多重要的定理是赫尔维茨 (Adolf Hurwitz, 1859-1919, 德国数学家) 发现的, 因此都名为赫尔维茨定理. 这一个在许多文献中称为赫尔维茨赋范除法代数定理, 甚至称为赫尔维茨 1,2,4,8 定理.——中译本注

取 A 的一个与整个 $\mathbf{O}$ 都正交的、范数为 1 的元素, 称它为 i, 于是 $\mathrm{i}^* = -\mathrm{i}$, 所以 $1 = \mathrm{i}^*\mathrm{i} = -\mathrm{i}^2$, 而 $\mathrm{i}^2 = -1$. 现在取由 i 和 A 中所包含的 $\mathbf{O}$ 所生成的代数. 经过一些代数运算, 就可以证明这个代数由形状为 $x + \mathrm{i}y$ 的元素构成, 这里的 x 和 y 属于 $\mathbf{O}$. 此外, 还可以证明 $x + \mathrm{i}y$ 和 $z + \mathrm{i}w$ 的乘积是 $xz - wy^* + \mathrm{i}(x^*w + zy)$, 这也正是凯莱–迪克森构造所给出的.

关于四元数和八元数的讨论, 有两个极好的资料: 一是 John Baez 的网页 http://math.ucr.edu/home/baez/octonions; 二是一本书, 即 Conway J H and Smith D A. *On Quaternions and Octonions: Their Geometry, Arithmetic and Symmetry.* Wellesley, MA: AK Peters, 2003

III.77 表 示
(Representations)

有限群[I.3 §2.1]G的线性表示就是一种使 G 的每一个元 g 都与一个由*向量空间*[I.3 §2.3]V 到其自身的线性映射 T_g 相联系的方法. 这种联系当然要反映 G 的群结构, 所以 T_gT_h 应该等于 T_{gh}, 而若 e 是 G 的恒等元, T_e 就应该是 V 的恒等映射.

线性表示的一个有用的侧面就是 V 的维数可以比 G 的大小小得多. 如果是这样, 则表示把关于 G 的信息以更加有效的方式打起包来. 例如, *交错群*[III.68]A_5 共有 60 个元, 却同构于正 20 面体的旋转对称群, 而可以看作是 $\mathbf{R}^3$ 的一个变换群 (也就是一个由 3×3 矩阵所成的群).

表示之所以有用的一个更基本的理由是, 每一个表示都可以分解成为一些"积木", [就是一些结构单元], 称为既约表示. 因此, 关于 G 的大量信息都可以从它的既约表示的少量基本的事实导出.

这些思想也可以推广到无限群, 而在*李群*[III.48 §1] 的情况下特别重要. 因为李群有微分结构, 所以, 有意义的表示, 即同态 $g \mapsto T_g$, 也会反映这个结构 (例如应该是可微的).

在条目*表示理论*[IV.9] 中将对表示作详细得多的讨论, 也请参看条目*算子代数*[IV.15 §2].

III.78 里 奇 流
(Ricci Flow)

陶哲轩 (Terence Tao)

里奇流是一个数学技巧, 它能够让我们任意取一个*黎曼流形* [I.3 §6.10], 并把它

的几何学光滑化, 使它看起来更加对称. 已经证明, 在了解这种流形的拓扑上, 它是一种有力的工具.

可以对任意维的黎曼流形来定义里奇流, 但是出于讲述的目的, 我们只限于 2 维流形 (即曲面) 的情况, 因为这种情况是容易看得见的. 从日常对于 3 维空间 $\mathbf{R}^3$ 的经验, 我们对许多曲面是很熟悉的, 例如球面、柱面、平面、环面 (就是汽车轮胎表面的那种曲面), 等等. 这是一种从外界来思考或者说外包地 (extrinsic) 思考曲面的方法, 就是把它看成一个更大的外包空间 (ambient space) 的子集合, 而在现在的情况, 外包空间就是 3 维的欧几里得空间 $\mathbf{R}^3$. 另一方面, 也可以取一种比较抽象的内蕴的方式来思考曲面, 就是考虑曲面上的点相互之间处于何种关系, 而不是考虑曲面上的点与任意外在的空间的关系 (例如克莱因瓶, 从内蕴的观点来看, 就是完全有意义的曲面, 但是不能从外包的 3 维欧几里得空间 $\mathbf{R}^3$ 来看它, 虽然如此, 却又可以从外包的 4 维欧几里得空间 $\mathbf{R}^4$ 来看它). 因此, 这两种观点在绝大多数情况下是等价的, 但是在这里, 采用内蕴的视角更加方便.

地球表面是曲面的一个好例子. 从外界来看, 它是 3 维空间 $\mathbf{R}^3$ 的一个子集合. 但是可以用图册 (atlas) 的方法 2 维地观察这个曲面. 图册就是许多区图 (maps 或 charts) 的集合, 一个区图把曲面的一个部分与 2 维平面的一部分等同起来. 一个图册只要有足够多的区图足以把原来的曲面覆盖起来, 这个图册就可以用来描述曲面了. 这种思考曲面的方法并不是完全内蕴的, 因为对这个曲面还可以有别的图册, 而它们也会稍有差别. 例如, 洛杉矶在一本地图册 [(图册和区图虽然是数学名词, 但是都是从地图学里借用的, 其含义也是自明的)] 里可能位于某一区图的边缘上, 而在另一本图册里, 则可能位于另一个区图里面. 然而, 有许多可以从一本图册看到的事实, 并不依赖于图册的选取. 例如从洛杉矶到悉尼的旅程一定要跨过至少一个大洋, [从什么图册来看都是这样]. 如果关于一个曲面的某一事实, 不依赖于图册的选取, 就说它是内蕴的或与坐标无关的. 我们将会证明, 里奇流就是曲面上的一个内蕴流, 为了定义它不需要任何关于区图或外包空间的任何知识.

我们已经非形式地描述了曲面也就是 2 维流形这个数学概念. 但是为了描述里奇流, 还需要一个更深奥的黎曼式的曲面 (也就是 2 维的赋有黎曼度量的流形 ①) 的概念. 就是说, 是一个附加了一个 (内蕴的) 对象的曲面, 这个对象就是黎曼度量 G, 它可以用来确定曲面上两点 x, y 的距离 $d(x, y)$, 也可以用来确定曲面上两条曲线 γ_1, γ_2 在其交点处所成的角 $\angle\gamma_1, \gamma_2$, 例如地球的赤道与任意经线都交于直角. 黎曼度量也可以用来确定曲面上任意集合 A(例如澳大利亚) 的面积 $|A|$. 距离、交角、面积, 这些概念必须要具有某些性质, 但是其中最重要的可以非形式地

① 原书作 Riemannian surfaces, 如果形式地译为黎曼的曲面, 就会与下一个条目的黎曼曲面混淆, 成为一个笑话. 实际上原书的意思是"赋有黎曼度量的曲面", 下文就作了这样的说明, 所以在此硬造了一个生僻的词, 以免误会.—— 中译本注

表述如下：黎曼式的曲面的几何学, 在小的距离尺度上, 必须非常接近欧几里得平面的几何学.

现在举一个例子, 使上面所说的可以看得更清楚, 在曲面 M 上取一点 x, 再取任意的正数 r 作半径. 因为黎曼度量 $\mathcal{G}$ 可以确定距离概念, 因此可以定义以 x 为心、r 为半径的圆盘 $B(x,r)$ 就是距 x 点的距离 $d(x,y)$ 小于 r 的 y 点的集合. 因为黎曼度量 $\mathcal{G}$ 可以确定面积的概念, 所以可以来讨论这个圆盘 $B(x,r)$ 的面积. 在欧几里得平面上, 这个圆盘的面积是 πr^2. 但是在黎曼式的曲面上就不一定如此了, 例如整个地球表面积是有限的, 地球表面上的任意圆盘的面积当然也是有限的, 但是当 r 趋于无穷时 πr^2 可以任意大. 然而, 我们确实要求的只是当 r 变小时, 面积越来越接近 πr^2, 换句话说, 要求圆盘面积与 πr^2 之比当 $r \to 0$ 时收敛于 1.

这就把我们引导到标量曲率 $R(x)$ 的概念. 在有些情况下, 例如对于球面, 一个小圆盘 $B(x,r)$ 的面积 $|B(x,r)|$ 确实稍小于 πr^2. 在这个情况下, 我们说曲面在 x 点具有正标量曲率. 在其他情况例如在鞍形曲面上, $|B(x,r)|$ 又稍大于 πr^2, 这时就说, 在 x 点处曲面有负标量曲率. 还有一些情况, 例如在柱面上, 小圆盘 $B(x,r)$ 的面积 $|B(x,r)|$ 就等于 (或者更高阶地接近于)πr^2, 这时就说曲面在 x 点有零标量曲率 (尽管从外包观点来看, 柱面作为 3 维空间的子集合确实是 “弯曲” 的). 注意, 在复杂的曲面上, 完全可能在曲面的某些点上, 具有正标量曲率, 在另一些点上具有负或零标量曲率. 在任意给定点, 标量曲率可以精确地用以下公式来定义：

$$R(x) = \lim_{r \to 0} \frac{\pi r^2 - |B(x,r)|}{\pi r^4/24}$$

(对于包含在外包空间里的曲面, 内蕴的标量曲率的概念几乎等同于外包的高斯曲率的概念, 对于什么是高斯曲率, 这里就不讨论了).

还可以把这个概念精确化为里奇曲率 $\mathrm{Ric}(x)(v,v)$ 的概念. 在圆盘 $B(x,r)$ 内考虑一个扇形, 即从 x 点发出的以单位向量 (即某个半径的方向)v 为中线, 而开口角度为 θ(按弧度计算) 的扇形 $A(x,r,\theta,v)$. 这个扇形是可以适当地定义的, 这在基本上是因为黎曼度量给了适当的距离和角度的定义. 在欧几里得空间里, 这个扇形的面积 $|A(x,r,\theta,v)|$ 等于 $\frac{1}{2}\theta r^2$. 但是在曲面上, 这个面积 $|A(x,r,\theta,v)|$ 可以稍小于 (或相应地稍大于)$\frac{1}{2}\theta r^2$. 在这些情况下, 我们说曲面在 x 点和 v 方向上, 有正的 (或相应有负的) 里奇曲率. 更精确一点, 有

$$\mathrm{Ric}(x)(v,v) = \lim_{r \to 0} \lim_{\theta \to 0} \frac{\frac{1}{2}\theta r^2 - |A(x,r,\theta,v)|}{\theta r^4/24}.$$

现在可以证明, 对于曲面来说, 这个比较复杂的曲率概念实际上是标量曲率的

一半：$\mathrm{Ric}(x)(v,v)=\frac{1}{2}R(x)$. 特别是, 方向 v 在 2 维里奇曲率中其实不起作用. 然而, 可以把上面说的概念推广到更高维去 (例如, 要对于 3 维流形定义标量曲率和里奇曲率, 就需要使用球体和立体角, 而不是圆盘和扇形, 还需要作其他调整, 例如把 πr^2 换成 $\frac{4}{3}\pi r^3$). 在更高维情况下, 里奇曲率比标量曲率更复杂, 例如在 3 维情况下, 一个点可能在某个方向上有正的里奇曲率, 而在另一个方向上有负的里奇曲率. 这意味着, 在前一个方向上, 一个很窄的扇形 "向内弯曲", 而在后一个方向上的一个很窄的扇形 "向外弯曲".

现在可以把里奇流非形式地描述为黎曼度量 $\mathcal{G}$ 在负里奇曲率方向上拉伸, 而在正里奇曲率的方向上压缩的过程. 弯曲的程度越大, 拉伸和压缩的过程也就越快. 拉伸和压缩的概念不在这里形式地加以定义, 但是它们把这个方向上的距离增加或减少. 距离概念改变了, 角度和体积也就会受到影响 (虽然在 2 维情况下里奇流是共形的, 就是说, 角度概念不受流的影响. 这一点与前面提到过的, 在 2 维情况下, 里奇曲率在各个方向都一样这件事是密切相关的). 现在里奇流可以简洁地用下面的方程来描述：

$$\frac{\mathrm{d}}{\mathrm{d}t}\mathcal{G}=-2\mathrm{Ric},$$

虽然不在这里精确地定义度量 $\mathcal{G}$ 对时间求导数是什么意思, 也不解释这个导数等于里奇曲率乘以 -2 是什么意思.

从原则上说, 在一个流形上可以对任意长的时间周期作里奇流. 但是在实际上 (特别是在正里奇曲率情况), 里奇流可能使一个流形发展出奇性, 就是发展成使得流形在一些点处看起来不再像是流形, 在这些地方, 流形的几何学哪怕在很小的尺度下也不再像是欧几里得几何学. 例如, 如果从一个完全滚圆的球面开始作里奇流, 则球面将以一定的速率收缩, 直到变成一个点, 这就不再是一个 2 维流形了. 在 3 维的情况还可能有更复杂的奇性, 例如可以有颈部挤压 (neck pinch) 就是流形有一个柱形的 "颈子", 在里奇流下压拢来, 而在一个或几个点处挤成了一个点. 在佩雷尔曼 (Grigori Perelman) 近来的一篇重要的文章里, 才对 3 维里奇流的可能的奇性形成的类型做出了完全的分类.

几年以前, 哈密顿 (Richard Hamilton, 1943—, 美国数学家) 看出了一个重要之点, 即里奇流是简化一个流形的构造的极佳的工具. 一般说来, 它能把流形的正曲率部分压缩成乌有, 而把负曲率部分放大, 直到使得这些部分变得非常均匀, 意思是不论在此流形选取哪个视点, 这个流形看起来都是一样的. 说真的, 里奇流好像是把流形分成了几个极为对称的分支. 例如在 2 维情况下, 里奇流总是终结为使得流形具有常曲率, 它可能为正 (好像球面)、为零 (好像柱面) 或者为负 (好像双曲空间), 在曲面理论中总能够找到这样的常曲率的度量, 这一事实以单值化定理 [V.34]

之名为人所知, 而有着基本的重要性. 在高维情况下, 里奇流在达到完全的对称性之前就已经发展出了奇性, 但是结果是有可能对这样发展出来的奇性作 "割补术"(surgery)(见条目*微分拓扑*[IV.7 §§2.3, 2.4]), 使得流形又重新变成光滑的, 而可以再次启动里奇流的过程 (但是, 割补会改变流形的拓扑, 例如可能把一个连通的流形分成不连通的几块). 在 3 维情况, 佩雷尔曼最近证明了, 里奇流再辅以割补术, 确实能把任意的流形 (当然要有一些不太强的假设) 分成有限块非常对称而且可以显式地加以描述的几块之并. 这个结论的精确的陈述, 就是人们所知道的瑟斯顿 (Thurston) 几何化假设. 这个假设有一个推论就是庞加莱猜想, 而由于佩雷尔曼的证明, 这个猜想现在已经是一个严格的定理了. *庞加莱猜想*[V.25] 宣称: 任意紧的单连通流形 (就是其上的任意闭环都可不必离开此流形而连续收缩为一点的流形) 都可以光滑地变形成为一个 3 维球面 (3 维球面在 4 维欧几里得空间里的地位, 就如通常的 2 维球面在 3 维欧几里得空间中的地位一样). 在当代数学中, 庞加莱猜想的证明是近来最给人以深刻印象的进展之一.

III.79 黎曼曲面
(Riemann Surfaces)

Alan E. Beardon

令 D 为复平面的一个区域 (即连通开集合). 如果 f 是定义在 D 上的复值函数, 则可以和定义在 $\mathbf{R}$ 的子集合上的实值函数的导数一样, 定义 f 在 $w \in D$ 处的导数为以下的 "差商"$(f(z)-f(w))/(z-w)$ 当 z 趋近 w 时的极限. 当然, 这个极限不一定存在, 但是如果它对 D 中的所有 w 点都存在, 则说 f 在 D 上解析或者全纯. 解析函数有惊人的性质, 例如, 如果一个函数在一区域中解析, 它在此区域的每一点都自动地有泰勒级数展开, 由此可以导出它必定无穷次可微. 这与实变量的实函数理论形成尖锐的对比, 在那里, 例如一个函数在某一点 x 一次可微, 但不是二次可微, 然而在另一点 y 又三次可微. 复分析就是对解析函数的研究, 它既在实际工作中有巨大的应用, 又在理论意义下深刻而且美丽, 就这一点来说, 可能超过任何其他的数学分支 (在 [I.3 §5.6] 中, 对复分析的某些基本结果作了介绍).

正如群论的专家对于互相同构的群不加区别、拓扑学家对于互相同胚的拓扑空间不加区别一样, 复分析专家对于两个区域 D 和 D', 如果它们之间有一个解析双射存在, 也就不加区别. 如果是这样的情况, 就说 D 和 D' 是共形等价的. 顾名思义, 共形等价是一个*等价关系*[I.2 §2.3], 这一点的证明依赖于一个惊人的事实, 即若 f 是一个由 D 到 D' 解析双射, 则其逆 $f^{-1}: D' \to D$ 也是解析的, 这又一次与实分析形成对照. 如果 D 和 D' 是共形等价的, 则在 D 上的解析函数的 "有趣的"

性质都自动地转移成 D' 上的解析函数的相应的性质. 事实上, 这个命题甚至可以取来作为所谓 "有趣的" 性质的定义 (虽然这里要承认这个 "定义" 与复分析的数值的侧面是有矛盾的, 因为 "有趣的" 数值性质, 通常并不会在这种映射下转移).

我们自然愿意知道解析函数的哪些性质在这个意义下是 "有趣的". 这种 "有趣的" 性质之一是: 在解析映射下, 两条在 D 中相交的曲线 (除非交点是 D 中某些孤立点) 的交角保持不变, "共形" 一词就是由此而来的. 但是下面的事实就不那么众所周知了: 如果一个双射 (不假设是可微的) 能够保持角不变 (就是角的大小和顺时针或逆时针都不变), 则它是解析的. 这样, 马虎一点就说保持角不变蕴含了泰勒级数存在!

复分析对其他分支影响如此巨大, 所以很自然地会去寻找可以在其上研究解析函数的最一般的曲面的类型, 这就引导到了黎曼曲面 (这样命名是为了纪念黎曼[VI.49], 他在自己的学位论文里引进了这个概念). 为了在曲面 S 上放上一个坐标系, 把 S 双射映到一个平面区域 D 上. 如果成功了, 就把 D 中的坐标转移到 S 上. 对于许多曲面 (例如球面), 是找不到这样的映射的, 所以只能满足于找一个局部坐标. 这就是说, 对于 S 上一点 w, 把它的一个邻域 N[双射地] 映到一个平面区域上, 于是得到一个限制在 N 中的坐标系, [这就叫做局部坐标]. 因为通常有无穷多种方法来引入局部坐标, 所以就不得不考虑所谓转移映射的类. 转移映射就是从 w 处的一个局部坐标到另一个局部坐标的映射. 如果每一个转移映射都是解析双射, 就说 S 是一个黎曼曲面. 这个定义很像一个 2 维流形[I.3 §6.9] 的定义, 但是转移映射必须是解析双射, 这个要求比对于一般流形的转移映射的要求是强多了, 所以绝非每一个 2 维流形都是黎曼曲面.

构造黎曼曲面并不算是很困难的事, 例如考虑一个放在水平的桌面上的球面. 想象有一个光源放在球面的最高点 P, 则球面上的每一点 S, 除非 S 就是 P, 都会在桌面上投下一个 "影子", 因为桌面上有简单的坐标系, 所以就能用这些影子, 在球面上定义一个坐标系, 但 P 点除外. 如果在球面与桌面的切点 Q 处放一个光源, 则又可以在球面的 P 点处的水平切面上投下一个影子, 这又给出了一个在球面上除在 Q 点都适用的坐标系. 可以证明, 如果把第二个坐标系与一个反射复合起来, 则球面得到了黎曼曲面的结构. 这是一个极为重要的例子, 因为它给出了涉及无穷远点的问题的一种令人满意的处理方法. 球面在有了这样的黎曼曲面结构以后, 就称为黎曼球面.

作为另一个例子, 考虑一个立方体 C 并且除掉它的 8 个顶点 (这完全是为简单起见). 给出立方体 C 的一个面 F(但是作为其边的棱要除掉), 可以找到一个欧几里得运动把 F 移到复平面 $\mathbf{C}$ 内, 这样就可以在 F 上定义一个坐标系. 如果 w 是立方体 C 的棱 E 的一个内点, 则可以把立方体 C 的在棱 E 上相遇的两个面 "摊平", 以得到一个包含 E 的平面区域, 然后再用一个欧几里得运动把这个平面区域

送到复平面 $\mathbf{C}$ 中. 这样就看到, 立方体 C(除去顶点) 也是一个黎曼曲面. 顶点产生的问题可以用技术手段来解决, 而这个方法可以推广来证明任意多面体 (甚至包括 "有洞" 的多面体, 如 "正方形环面") 都是黎曼曲面, 这些曲面都是紧曲面. 有一个深刻而有魅力的经典结果宣称, 这些黎曼曲面双射地相应于一个既约的二复变量多项式 $P(z,w)$. 为了对这种对应关系给出一点印象, 考虑方程 $w^3+wz+z^2=0$. 对于每一个 z 可以从这个方程解出 3 个 w 来, 例如记为 w_1,w_2,w_3; 当 z 在复平面 $\mathbf{C}$ 上变动时, 这些 w_j 也就在变动, 而生成一个黎曼曲面 W, 可以证明它是连通的. 可以想象 W 位于复平面 C 的 "上方", 而对复平面 $\mathbf{C}$ 的所有的 z 点, 最多除有限个 z 例外, 总有恰好 3 个 W 的点位于这个 z 的 "正上方".

如已经提到的那样, 黎曼曲面是可以在其上研究解析函数及其所有值得注意的性质的最一般的曲面. 很容易定义什么是我们所谓的黎曼曲面 R 上的解析函数 f. f 是坐标的函数, 而我们认为 f 是解析的, 当且仅当它解析地依赖于这些坐标. 由于转移映射是解析的, 所以 f 对于一个坐标系为解析的, 当且仅当 f 对于所有定义在这一点附近的坐标系均为解析.

这样一个简单的性质 —— 如果某事对一个坐标系成立, 则必对所有坐标系成立 —— 是这个理论的一个关键性的特性. 例如, 设有两条曲线在某个 (抽象的) 黎曼曲面上相交. 如果用不同的局部坐标系把这两条曲线转移到复平面上去, 然后在每一个情况下量它们的交角, 就一定会得到相同的结果 (因为从一个坐标系到另一个坐标系的转移映射保持角不变). 由此可知, 在抽象的黎曼曲面上, 两条曲线的交角是一个有适当定义的概念.

后来还发现, 黎曼曲面上的分析可以越出解析函数的范围. 调和函数 (即*拉普拉斯方程*[I.3 §5.4] 的解) 与解析函数有密切联系, 因为一个解析函数的实部一定是调和函数, 而一个调和函数一定也 (局部地) 是一个解析函数的实部. 这样, 在黎曼曲面上, 复分析不知不觉地和位势理论 (也就是调和函数的研究) 融合在一起了.

在关于黎曼曲面的所有定理中, 最深刻的说不定就是*单值化定理*[V.34] 了. 粗略地说, 这个定理说的就是: 每一个黎曼曲面都可以从欧几里得几何、球面几何或双曲几何 (见条目*一些基本的数学定义*[I.3 §§6.2, 6.5, 6.6]) 按下面的方法得出. 取相应几何学的一个多边形, 并把它的各边按适当的方法粘贴在一起, 就如同我们曾经把矩形的对边粘贴起来并得出环面那样 (亦见条目*富克斯群*[III.28]). 值得注意的是, 只有很少的黎曼曲面来自欧几里得几何或球面几何. 本质上说, 所有的黎曼曲面都来自 (而且仅仅来自) 双曲平面. 这意味着复平面的几乎每一个区域都带有自然的内蕴的几何学, 它的特性是双曲的, 而不是如我们所想象的那样是欧几里得的. 通常的平面区域的欧几里得性质来自它是嵌入在复平面 $\mathbf{C}$ 中, 而不是来自它的内蕴的双曲几何学.

III.80 黎曼 ς 函数
(The Riemann Zeta Function)

黎曼 ς 函数是一个复变量的函数, 它以非常值得注意的方式把有关素数的分布的许多性质包含在自身中. 如果 s 是一个实部大于 1 的复数, 则需要满足 $\mathrm{Re}(s) > 1$ 这个条件才能把 $\varsigma(s)$ 定义为 $\sum_{n=1}^{\infty} n^{-s}$. 这个条件的作用是为了保证这个级数收敛. 然而由于所得到的函数是*全纯函数*[I.3 §5.6], 所以可以用解析拓展来扩张这个定义. 结果, 黎曼 ς 函数就在复平面上处处有定义 (虽然在 $s = 1$ 处的值是 ∞).

为什么这个函数与素数的分布有关? 第一个线索是欧拉的乘积公式:

$$\varsigma(s) = \prod_p (1 - p^{-s})^{-1},$$

右方的乘积是对所有的素数 p 取的. 这个公式可以这样来证明, 就是把 $(1 - p^{-s})^{-1}$ 写成 $1 + p^{-s} + p^{-2s} + \cdots$, 再应用*算术的基本定理*[V.14]. 更深刻的联系是由*黎曼*[VI.49] 发现的, 他提出了著名的*黎曼假设*[IV.2 §3].

黎曼 ς 函数只是一族记载了重要的数论的信息的函数之一. 例如狄里克莱 L 函数就与算术数列中素数的分布有密切的关系. 关于这些问题和更多的关于黎曼 ς 函数的细节, 请参看条目*解析数论*[IV.2], 有些更深奥的 ς 函数在条目*韦伊猜想*[V.35] 中会讲到, 也可参看条目 *L 函数*[III.47]

III.81 环, 理想与模
(Rings, Ideals, and Modules)

1. 环

*环*和*群*[I.3 §2.1]、*域*[I.3 §2.2] 一样, 都是一种满足某些公理的代数结构. 想要同时记住环和域的公理, 想两个简单的例子是有帮助的, 这两个例子中都有加法和乘法两种运算: 其一是所有整数的集合 $\mathbf{Z}$, 它是一个环; 其二是所有有理数的集合 $\mathbf{Q}$, 它是一个域. 一般说来环就是一个具有两个*二元运算*[I.2 §2.4] 的集合 R, 这两个运算记作 "+" 和 "×", 它们满足其在域中的所有公理, 只有一个除外, 就是非零元素必有乘法逆这一条不一定成立.

虽然整数集合是环的一个原型例子, 但是从历史上看, 这个概念却是从几个来源抽象出来的, 其中之一就是多项式. 多项式 (例如说是实系数的) 可以相加和相

乘, 所有这些运算都有我们可以期望的性质, 例如乘法对于加法是分配的, 所以多项式的空间也构成一个环. 其他的例子还有整数 mod$n$(n 是任意正整数)、有理数 (其实任意其他的域都是) 和所有形如 $a+\mathrm{i}b(a,b$ 是整数) 的复数的集合 $\mathbf{Z}(\mathrm{i})$.

[在环的公理中], 有时会把乘法的可交换性以及乘法有恒等元存在这两条去掉. 这会使得理论变得复杂一些, 但是仍然包含了重要的例子, 如所有 $n\times n$ 矩阵 (其元素在一个域中, 甚至只在一个环中) 的集合.

和其他的代数结构一样, 有好几种从原有的环作出新环的方法, 可以取子环或两个环的直积. 不那么明显的则有: 从一个环 R 开始, 再作系数在 R 中的多项式, 所有这些多项式也构成一个环. 还可以取商[I.3 §3.3], 但是, 要讨论这些, 就需要理想的概念.

2. 理想

对于代数结构 A, 构造一个商的典型的方法就是确定一个子结构 $B\subset A$, 而 A 中的两个元, "如果只相差一个 B 中之元" 就认为它们是 "等价的". 如果 A 是一个群或者向量空间[I.3 §2.3], 则 B 应取为一个子群或子空间. 然而, 环的情况则稍有不同.

如果从另一个角度来看商结构, 就会明白为什么会这样, 这就是从同态[I.3 §4.1] 的像的角度来看这个问题. 我们将用这些同态的核作为子结构 B, 再来作 A 对于 B 的商, 所以我们要问: 环同态的核 (即被映射为 0 的元素的集合) 怎样.

如果 $\phi:R\to R'$ 是两个环 R 和 R' 之间的同态, 而且 $\phi(a)=\phi(b)=0$, 则 $\phi(a+b)=0$, 就是说, 同态的核在环的加法下是封闭的. 此外, 如果 $r\in R$ 是环 R 的任意元 [但不一定是同态核中的元], 仍有 $\phi(ra)=\phi(r)\phi(a)=0$, 就是说这个同态核在乘以环中任意元 [而不一定限于乘以这个核中的元] 的乘法下也是封闭的. 这两个性质给出了理想的定义. 举一个例子, 所有偶数的集合是整数环 $\mathbf{Z}$ 的理想. 在许多有趣的情况下, 理想不是子环, 因为如果一个理想含有环的乘法单位元 1, 则它应该包含环中的任意元 (有一个例子足以说清楚子环和理想的区别, 考虑多项式环的由常数多项式 —— 即常数本身 —— 所成的子集合, 它肯定是一个子环, 但显然不是一个理想).

不难证明, 对于环 R 的任意理想 I, 必可找到一个同态, 使得 I 恰好是这个同态的核. 具体地说, 这个同态就是从 R 到 R/I 的商映射. 这里 R/I 就是我们通常这样来想的结构: "R 中的两个元素, 如果只相差一个 I 中的元素, 就认为是相同的."

环的商在代数数理论[IV.1] 中极为有用, 因为它使得我们能够把关于代数数的问题重新陈述为关于多项式的问题. 为了对于这是怎么回事有点印象, 考虑具有整数系数的多项式所成的环 $\mathbf{Z}[X]$ 以及它的一个由 X^2+1 的 "倍"(就是 X^2+1 乘以任意整系数多项式) 所构成的理想. 在 $\mathbf{Z}[X]$ 关于这个理想的商中, 我们认为两个只

相差 X^2+1 的一个倍的多项式是相同的, 特别是 X^2 和 -1 将被认为是相同的. 换言之, 在此商环里有 -1 的平方根, 事实上, 这个商环就同构于前面遇到的环 $\mathbf{Z}[\mathrm{i}]$.

对于整数, 我们愿意做的一件事情是分解因子, 而我们可以试着对环也做这件事情. 然而情况是, 虽然环中的元素可以分解为不能再进一步分解的 "既约元素"(像 $\mathbf{Z}$ 中的素数那样), 但在许多情况下, 这种分解并不是唯一的. 一开始, 这似乎是意想不到的事, 后来却成了许多 (18 和 19 世纪的) 早期研究者的绊脚石. 下面是一个例子, 在环 $\mathbf{Z}\left[\sqrt{-3}\right]$(由形如 $a+b\sqrt{-3}, a, b$ 为整数的数构成) 中, 4 这个数, 既可以分解成 2×2, 也可以分解成 $(1+\sqrt{-3})(1-\sqrt{-3})$.

3. 模

模之于环, 就如同向量空间之于域. 换句话说, 模是这样的代数结构, 其中有两个运算, 一是加法, 一是用标量去乘它的一个元, 但是现在标量可以来自一个环, 而不一定来自一个域. 举一个环上的但不是域上的模的例子. 取任意阿贝尔群 G, 可以把它变成环 $\mathbf{Z}$ 上的模, 其中的加法就是群运算, 而用标量来求一个元的倍, 则可以用显然的方法来定义, 例如 $3g$ 定义为 $g+g+g$, 而 $-2g$ 则定义为 $g+g$ 的逆.

定义如此简单, 却掩盖了一件事实, 就是模的结构, 一般说来, 比向量空间的结构要微妙得多. 例如模的基底也可以定义为其中一组线性无关却张成整个模的元素的集合. 然而, 向量空间的关于基底的许多有用的性质在模中并不成立. 例如, $\mathbf{Z}$ 可以看作在其本身上的模, 集合 $\{2,3\}$ 张成整个 $\mathbf{Z}$ 但是并不包含它的一个基底, [因为它们并非线性无关的, $3\times 2+(-2)\times 3=0$]; 集合 $\{2\}$ 是线性无关的, 但是不能扩展成基底. 事实上, 远非每一个模都有基底, 例如把 $\bmod n$ 的整数集合看成 $\mathbf{Z}$ 上的模, 则哪怕是单个的元 x 也不是线性无关的, 因为 $nx=0$.

下面的例子是一个重要的模. 令 V 为一个复向量空间, 而 α 是一个从 V 到 V 的线性映射. V 可以作成一个环 $\mathbf{C}[X]$(即复系数多项式环) 上的模如下: 若 $v\in V$, 而 P 是一个复多项式, 定义 Pv 为 $P(\alpha)v$(例如, 设 P 为多项式 X^2+1, 则 $Pv=\alpha^2v+v$). 应用关于模的一般结构的定理, 就可以得到约当法式定理[III.43] 的一个证明.

III.82 概　型
(Schemes)

Jordan S. Ellenberg

数学史上常有这样的事: 一个定义原来觉得已经是完全一般的了, 但是在处理感兴趣的问题时, 又发现仍然过于局限. 例如, "数" 的概念已经一再地扩展了 —— 最值得注意的是, 把无理数和复数都包括进来了. 前者来自几何学, 后者则是求解任意的代数方程之所需. 类似于此, 代数几何学, 原来的了解是为了研究代数簇,

就是研究有限维空间中的代数方程组的解集合, 后来发展到把更一般的对象也包括进来了, 这就是"概型"(scheme). 作为一个很不足道的例子, 可以考虑两个方程 $x+y=0$ 和 $(x+y)^2=0$. 它们在平面上有相同的解集合, 所以描述同样的簇, 但是与这两个对象相联系的概型却完全不同. 用概型的语言来重述代数几何学是由格罗滕迪克 (Alexander Grothendieck) 在 1960 年代开创的一个宏大的计划. 如上例所示, 概型论的观点想要强调的是这个主题 (方程) 的代数的侧面, 而不是传统的几何侧面 (方程的解集合). 这个观点使得人们长久期望着的*代数数理论*[IV.1] 与代数几何学的统一成了现实, 而事实上, 近年来数论的大量进展, 如果没有概型理论提供的几何洞察, 也是不可能的.

甚至概型也还不足以解决当前人们感兴趣的所有问题, 而更一般的概念 (如栈 (stack)①、"非交换簇"、束的导出范畴 (derived category of sheaves) 等等) 在有必要时也都会用上. 所有这些, 看起来都有点怪, 但是对于后人, 它们也都会是第二天性, 正如概型对于我们一样. 关于代数几何学的一般介绍, 可见条目*代数几何*[IV.4]. 关于概型, 则在条目*算术几何*[IV.5] 中作了较详细的讨论.

III.83 薛定谔方程 (The Schrödinger Equation)

陶哲轩 (Terence Tao)

在数学物理中, 薛定谔方程 (以及密切相关的海森堡方程) 是非相对论量子力学最基本的方程, 其作用犹如哈密顿方程 (以及泊松方程) 在非相对论的经典力学中的作用 (在相对论的量子力学中, 量子场论的方程取代了海森堡方程, 而薛定谔方程则没有直接的类比). 在纯粹数学中, 薛定谔方程以及它的变体是*偏微分方程*[IV.12] 这个研究领域中基本的方程之一, 而对于几何学、谱和散射理论以及可积系统都有应用.

薛定谔方程可以用来描述多粒子系统在各种力的影响下的量子动力学. 但是为简单计, 只考虑单个质量为 $m>0$ 的粒子在位势 ∇ 的作用下在 n 维空间 $\mathbf{R}^n$ 中的运动, 而位势则取为一个函数 $V:\mathbf{R}^n\to\mathbf{R}$. 为了绕过技术性的细节, 假设所有考虑的函数都是光滑的.

在经典力学中, 粒子在每一时刻 t 都有确定的位置 $q(t)\in\mathbf{R}^n$ 以及确定的动量 $p(t)\in\mathbf{R}^n$(我们终于会看到熟知的定律: $p(t)=mv(t)$, 这里 $v(t)=q'(t)$ 是粒子的速度). 这样, 这个系统在任意时刻 t 的状态将由空间 $\mathbf{R}^n\times\mathbf{R}^n$(称为相空间) 的元素 $(q(t),p(t))$ 来表示. 这个系统的能量则由相空间上的*哈密顿函数*[III.35]H:

① stack 一词没有找到合适的中文译名, 暂译为"栈". —— 中译本注

$\mathbf{R}^n \times \mathbf{R}^n \to \mathbf{R}$ 来表示. 在我们的情况下, 哈密顿函数由下式定义:

$$H(q,p) = \frac{|p|^2}{2m} + V(q)$$

(在物理上, $|p|^2/2m$ 表示动能, 而 $V(q)$ 表示位能). 然后这个系统, 就依照哈密顿运动方程

$$q'(t) = \frac{\partial H}{\partial p}, \quad p'(t) = -\frac{\partial H}{\partial q} \tag{1}$$

演化. 这里要记住, p 和 q 都是向量, 所以上式里的偏导数都是*梯度*[I.3 §5.3]. 哈密顿运动方程对于任意经典系统都有效, 而在特定的 "势阱" 中的粒子的情况下, 这个方程组成了

$$q'(t) = \frac{1}{m}p(t), \quad p'(t) = -\nabla V(q). \tag{2}$$

这里的第一个方程就是确定了 $p = mv$, 而第二个方程基本上就是牛顿的第二运动定律.

由 (1) 可以容易地导出泊松运动方程, 就是对每一个经典的可观测量 $A : \mathbf{R}^n \times \mathbf{R}^n \to \mathbf{R}$,

$$\frac{\mathrm{d}}{\mathrm{d}t}A(q(t), p(t)) = \{H, A\}(q(t), p(t)), \tag{3}$$

这里

$$\{H, A\} = \frac{\partial H}{\partial p}\frac{\partial A}{\partial q} - \frac{\partial H}{\partial q}\frac{\partial A}{\partial p}$$

是 H 和 A 的泊松括弧. 特别是若令 $A = H$, 就得到能量守恒定律:

$$H(q(t), p(t)) = E, \tag{4}$$

此式在所有时间 t 都成立, 而 E[在轨道上取与时间 t 无关的常值, 但这个常值即总能量. 在不同轨道上是粒子的总能量不相同的].

现在分析这个经典力学系统在量子力学中的类比. 这时需要一个正的小参数 $\hbar > 0$, 称为普朗克 (Planck constant) 常数①. 现在粒子的状态不再由相空间的一点 $(q(t), p(t))$ 来表示, 而是用一个波函数来表示, [所以, 波函数就是一个粒子的量子态]. 波函数是位置的复值函数, 它随时间演化. 就是说, 在每一个时刻 t 都有一个函数 $\psi(t) : \mathbf{R}^n \to \mathbf{C}$. 我们要求波函数满足规范化条件 $\langle \psi(t), \psi(t) \rangle = 1$, 这里 $\langle \cdot, \cdot \rangle$ 表示厄尔米特内积

$$\langle \phi, \psi \rangle = \int_{\mathbf{R}^n} \phi(q)\,\overline{\psi(q)}\mathrm{d}q.$$

---

① 在许多应用中, 都把 $\hbar$ 和 m 规范化为 1.

实际上, 这个 $\hbar$ 应称为化约普朗克常数 (reduced Planck constant), 有的文献也称它为狄拉克常数, 它的值是 $1.054571628(53) \times 10^{-34}\,\mathrm{J \cdot s}$, 而与普朗克常数 $h = 6.626068 \times 10^{-34}\,\mathrm{J \cdot s}$ 的关系是 $\hbar = h/2\pi$.——中译本注

和经典粒子不同, 量子粒子并没有一个确定的位置, 然而却有一个平均位置 $\langle q(t)\rangle$, 定义为

$$\langle q(t)\rangle = \langle Q\psi(t), \psi(t)\rangle = \int_{\mathbf{R}^n} q\left|\psi(t,q)\right|^2 \mathrm{d}q.$$

这里使用了记号 $\psi(t,q)$ 表示波函数 $\psi(t)$ 在 q 点的值, 而 Q 则是位置算子, 其定义为 $(Q\psi)(t,q) = q\psi(t,q)$, 就是说 Q 就是逐点乘以 q 这个算子. 类似地, 虽然量子粒子没有确定的动量, 却有平均动量 $\langle p(t)\rangle$, 定义为

$$\langle p(t)\rangle = \langle p\psi(t), \psi(t)\rangle = \frac{\hbar}{\mathrm{i}}\int_{\mathrm{R}^n} (\nabla_q\psi(t,q))\overline{\psi(t,q)}\mathrm{d}q,$$

其中的动量算子 P 则由普朗克定律来定义:

$$P\Psi(t,q) = \frac{\hbar}{\mathrm{i}}\nabla_q\Psi(t,q).$$

注意, 向量 $\langle p(t)\rangle$ 是实向量, 因为动量算子的各个分量都是自伴[III.50 §3.2]的 [在量子力学中所谓量子可观测量], 就是作用在复值勒贝格平方可积函数空间 $L^2(\mathbf{R}^n)$ 上的一个自伴算子[III.50]A. 可以定义它在量子态 ψ 和时刻 t 的平均值 $\langle A(t)\rangle$ 为

$$\langle A(t)\rangle = \langle A\psi(t), \psi(t)\rangle.$$

哈密顿运动方程 (1) 在量子力学中的类似物现在就是时变的 (time-dependent) 薛定谔方程

$$\mathrm{i}\hbar\frac{\partial\Psi}{\partial t} = H\Psi, \tag{5}$$

不过现在 H 是一个量子可观测量, 而不是经典的可观测量. 确切一点说, 就是

$$H = \frac{|p|^2}{2m} + V(Q).$$

换言之, 现在有

$$\begin{aligned}\mathrm{i}\hbar\frac{\partial\psi}{\partial t}(t,q) &= H\psi(t,q)\\ &= -\frac{\hbar^2}{2m}\Delta_q\psi(t,q) + V(q)\psi(t,q),\end{aligned}$$

其中

$$\Delta_q\psi = \sum_{i=1}^{n}\frac{\partial^2\psi}{\partial q_i^2}$$

是拉普拉斯算子作用在 ψ 上. 泊松运动方程 (3) 的类比则是海森堡方程, 即对任意的量子可观测量均有

$$\frac{\mathrm{d}}{\mathrm{d}t}\langle A(t)\langle = \left\langle\frac{\mathrm{i}}{\hbar}[H(t), A(t)]\right\rangle \tag{6}$$

这里 $[A,B]=AB-BA$ 是 A 和 B 的交换子或称李括弧 (量 $(\mathrm{i}/\hbar)[A,B]$ 有时也称为 A 和 B 的量子泊松括弧).

如果量子态 ψ(也就是波函数) 按下式随时间振动: $\psi(t,q)=\mathrm{e}^{(E/\mathrm{i}\hbar)t}\psi(0,q)$, 这里 E 是一个实数 (即所谓能级或本征值), 则将得到与时间无关的薛定谔方程 (或译为 "时齐的薛定谔方程"):

$$H\psi(t)=E\psi(t)\,\text{对一切时间成立} \tag{7}$$

(请将此式与 (4) 式比较). 一般说来, 谱论这个重要的分支 (见条目谱[III.86]) 将会提供与时间无关的薛定谔方程 (7) 与时变的薛定谔方程 (5) 的许多联系.

经典力学的方程与量子力学的方程有几个很强的类比. 例如, 由 (6) 可得

$$\frac{\mathrm{d}}{\mathrm{d}t}\langle q(t)\rangle=\frac{1}{m}\langle p(t)\rangle,\quad \frac{\mathrm{d}}{\mathrm{d}t}\langle p(t)\rangle=-\langle\nabla_q V(q)(t)\rangle,$$

请把它们与 (2) 比较. 还有, 得到了哈密顿运动方程的经典的解 $t\mapsto(q(t),p(t))$, 就可以作出薛定谔方程的相应的一族近似解 $\psi(t)$, 例如可以通过以下的公式来做 ①:

$$\psi(t,q)=\mathrm{e}^{(\mathrm{i}/\hbar)L(t)}\mathrm{e}^{(\mathrm{i}/\hbar)p(t)\cdot(q-q(t))}\varphi(q-q(t)),$$

其中

$$L(t)=\int_0^t\left[\frac{p(s)^2}{2m}-V(q(s))\right]\mathrm{d}s$$

是经典的作用量, 而 φ 是任意的服从以下规范条件的缓变函数

$$\int_{\mathbf{R}^n}|\phi(q)|^2\,\mathrm{d}q=1.$$

可以验证, 上式确实给出了薛定谔方程 (5) 的一个近似解, 而且当 $\hbar$ 很小时, 误差也很小. 这个事实是量子力学的所谓对应原理 (correspondence principle) 的一个例子. 这个原理说的是因为 $\hbar$ 很小, 所以, 在宏观尺度下工作时, 经典力学就可以用来准确地逼近量子力学 (上面可以应用任意缓变的 φ, 正是因为这个理由). 在数学中 (更确切地说是在微局部分析 (microlocal analysis) 和半经典分析 (semi-classical analysis) 这些领域中), 这个原理有好几种形式化, 使我们能用关于哈密顿运动方程的知识来分析薛定谔方程. 例如, 如果经典的运动方程有周期解, 则薛定谔方程时

① 直观地说, 函数 $\psi(t,q)$ 位置上局部化于 $q(t)$ 附近, 动量上则局部化于 $p(t)$ 附近, 所以在相空间中局部化于 $(q(t),p(t))$ 附近. 这样一个局部化的函数展现了 "类似粒子的" 性态, 即具有合理地确定的位置和动量, 所以有时称为 "波包". 薛定谔方程典型的解、形态并不像一个波包, 但是可以分解为波包的叠加, 即线性组合, 这种分解在研究这种方程时是一个有力的工具.

常也有近周期解, 而如果经典的方程有非常混沌的解, 则薛定谔方程典型地也是这样 (这个现象称为量子混沌或量子遍历性).

薛定谔方程有许多有趣的侧面. 我们只提出一个作为例子, 就是散射理论. 如果位势函数 V 在无穷远处衰减充分快, 而 $k \in \mathbf{R}^n$ 是一个非零频率向量, 则与时间无关的薛定谔方程 $H\psi = E\psi$ 有解 ψ, 这里 $E = \hbar^2 |k|^2 / 2m$, 是能级, 而其渐近性态 (即当 $|q| \to \infty$ 时) 为

$$\psi(q) \approx \mathrm{e}^{\mathrm{i}k \cdot q} + f\left(\frac{q}{|q|}, k\right) \frac{\mathrm{e}^{\mathrm{i}|k||q|}}{r(n-1)/2},$$

f 是某个典则函数 $f : S^{n-1} \times \mathbf{R}^n \to \mathbf{C}$, 称为散射振幅函数. 散射振幅函数 (非线性地) 依赖于位势函数 V, 而由位势函数 V 到散射振幅 f 的变换, 称为散射变换. 它可以看成是傅里叶变换[III.27] 的非线性变体, 它与偏微分方程的许多领域, 例如可积系统等均有联系.

薛定谔方程有许多推广和变化. 我们可以把它推广到多粒子系统, 或者加上其他的力如电磁场甚至非线性项. 也可以把这个方程与其他的物理方程, 如电磁理论的麦克斯韦方程[IV.13 §1.1] 耦合起来, 或者用其他空间如环面、离散格网或者流形来代替 $\mathbf{R}^n$, 另一方面, 又可以把不可贯穿的障碍物放进区域里 (从而把这些区域有效地从我们考虑的区域中除去). 所有这些变体引导到纯粹数学和数学物理的广阔而又多样的领域.

III.84 单 形 算 法
(The Simplex Algorithm)

Rucgard Weber

1. 线性规划

单形算法是解决出现在商业、科学和技术中一些最重要的数学问题的杰出的方法. 在这些总称为线性规划的问题里, 都要求使一个服从某些线性约束的线性函数达到最大 (或最小). 美国空军在 1947 年提出的伙食问题就是一个例子, 要求找出 77 种价格不同的食料 (如乳酪、菠菜等等) 各取多少, 使得既能满足一个人对于 9 种营养成分 (如蛋白质、铁等等) 的每日最低需求, 而又使成本最低. 在选择投资组合、安排飞机机组的名单以及选择二人对策中的最佳策略等方面还可以找到其他例子. 线性规划的研究导出了优化理论的中心思想, 例如对偶性[III.19]、凸性的重要性以及计算复杂性[IV.20] 等等.

线性规划 (以下简称为 LP) 的输入数据包括两个向量 $b \in \mathbf{R}^m, c \in \mathbf{R}^n$ 以及一个 $m \times n$ 矩阵 $A = (a_{ij})$. 问题则是找出 n 个非负的决定变量 $x_1, \cdots, x_n$([我们用一个行向量 x 来表示它]) 之值, 使目标函数 ([以下记作 $c^{\mathrm{T}}x, c = (c_1, \cdots, c_n)$])$c_1x_1 + \cdots + c_nx_n$ 达到最大, 但是这些变量 $x_1, \cdots, x_n$ 要服从 m 个约束条件 $a_{i1}x_1 + \cdots + a_{in}x_n \leqslant b_i, i = 1, \cdots, m$. 在伙食问题中, $n = 77, m = 9$. 而在下面的简单问题 (不是伙食问题) 中, $n = 2, m = 3$, 使 $x_1 + 2x_2$ 最大, 但要求

$$\begin{aligned} -x_1 + 2x_2 &\leqslant 2, \\ x_1 + x_2 &\leqslant 4, \\ 2x_1 - x_2 &\leqslant 5, \\ x_1, x_2 &\geqslant 0. \end{aligned}$$

在许多来自实际生活的问题中, n 和 m 可能比 100 000 还大.

这些约束对于 (x_1, x_2) 定义了一个可行区域. 这是一个凸多边形, 即图 1 上的阴影区域 "P". 图上的两条虚线标记出那些使得目标函数之值为 4 或为 6 的 x 点. 很明显, 目标函数在 C 点达到最大.

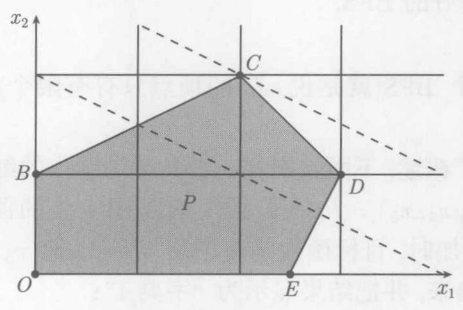


图 1 一个 LP 的可行区域"P"

一般的道理和这个例子是一样的. 如果可行区域 $P = \{x : Ax \leqslant b, x \geqslant 0\}$ 是非空的, 则它是 $\mathbf{R}^n$ 中的一个凸多胞形 (polytope), 而最优解可以在它的一个顶点上找到. 引入一些 "松弛变量"$x_3, x_4, x_5 \geqslant 0$ 来把约束不等式的左方 "放松" 是有好处的. 这样, 就可以把约束写成

$$\begin{aligned} -x_1 + 2x_2 + x_3 &= 2, \\ x_1 + x_2 + x_4 &= 4, \\ 2x_1 - x_2 + x_5 &= 5, \end{aligned}$$

现在就有了三个含有 5 变量的方程组, 所以, 可以令 $x_1, \cdots, x_5$ 中的任意两个为 0, 而从这 3 个方程中求出其余 3 个变量 (而当这 3 个方程碰巧不独立时, 则可以把方程组略加扰动然后来求解). 从 5 个变量中取 2 个, 共有 10 个取法, 并不是这 10 个解都适合条件 $x_1, x_2, x_3, x_4, x_5 \geqslant 0$, 但其中的 5 个确实满足这个条件. 这 5 个解

就叫做基本可行解 (简记为 BFS), 它们相应于图 1 上的 P 的顶点 O, B, C, D, E.

2. 这个算法如何运作

丹齐格 (George Dantzig) 在 1947 年发明了单形算法, 作为解决本文开始处提到的美国空军伙食问题的手段. "线性规划"(linear programming) 一词中的 program 现在都译为 "程序", 专指计算机的程序, 但是当时还没有这样的说法, 而是指的关于后勤的计划、安排等等, 是一个军事用语, 通常都译为 "规划". 这个算法依赖于一个基本的事实, 即若一个 LP 有一个有界的最优解, 则这个最优值一定产生在一个 BFS 上, 就是在可行点的多胞体 P 的一个顶点 (所谓的 "极端点") 上. 可行多胞体又名 "单形", 单形算法这个名称就是由此得来的. 单形算法是这样运作的:

第 0 步: 取一个 BFS.

第一步: 看这个 BFS 是否最优的.

　如果 "是", 停机;

　如果 "否", 转到下一步.

第二步: 求一个较好的 BFS.

重复第一步.

因为只有有限多个 BFS(就是说, P 的顶点只有有限个), 这个算法终究会停下来.

既已对此算法作了概述, 下面就来看一看具体的运作的细节. 设在第 0 步取的 BFS 是 $x = (x_1, x_2, x_3, x_4, x_5) = (0, 0, 2, 4, 5)$, 就是图 1 上的顶点 O. 第一步就是要看当 x_1 或 x_2 从 0 增加时, 目标函数是否增加. 所以, 把 x_3, x_4, x_5 以及目标函数 $c^{\mathrm{T}}x$ 都用 x_1, x_2 表示出来, 并把结果显示为 "字典 1":

字典 1

$$x_3 = 2 + x_1 - 2x_2$$
$$x_4 = 4 - x_1 - x_2,$$
$$x_5 = 5 - 2x_1 + x_2,$$
$$c^{\mathrm{T}}x = x_1 + 2x_2$$

字典的最后一行表明, 可以通过增加 x_1 或 x_2 来增加目标函数 $c^{\mathrm{T}}x$ 之值. 让我们增大 x_2, [而让 x_1 停留在 0 处]. 第一和第二个式子表明这时 x_3 和 x_4 必定减少. 但是我们不能把 x_2 增加得超过 1, [否则 x_3 会变成负的], 当 $x_2 = 1$ 时, [记住 $x_1 = 0$], 即有 $x_3 = 0, x_4 = 3, x_5 = 6$. 像这样尽可能地增加 x_2, 就会达到新的 BFS: $x = (0, 1, 0, 3, 6)$, 它就是图 1 中的顶点 B. [选取这个新的 BFS, 就是再次重复了第 0 步], 所以现在再来做第 1 步. 这里有两个变量 x_1 和 x_3 为 0 了, 于是就把

其余变量和目标函数用 x_1 和 x_3 写出来，从而得到字典 2：

字典 2	字曲 3
$x_2=1+\frac{1}{2}x_1-\frac{1}{2}x_3$	$x_1=2+\frac{1}{3}x_3-\frac{2}{3}x_4$
$x_4=3-\frac{3}{2}x_1+\frac{1}{2}x_3,$	$x_2=2-\frac{1}{3}x_3-\frac{1}{3}x_4$
$x_5=6-\frac{3}{2}x_1-\frac{1}{2}x_3$	$x_5=3-x_3+x_4,$
$c^{\mathrm{T}}x=2+2x_1-x_3$	$c^{\mathrm{T}}x=6-\frac{1}{3}x_3-\frac{4}{3}x_4.$

这说明如果让 x_1 增大，[但 x_3 保持为 0 不变]，则目标函数 $c^{\mathrm{T}}x$ 也将会增加. 这样令 x_1 由 0 增大到 2，这时 $x_4=0$. x_1 不能再增大了，否则 x_4 又会变成负的. 于是到达 P 的顶点 C，即一个新的 BFS $(2,2,0,0,3)$. 这样又一次完成了第 0 步，而可以再进行第 1 步了. 这样，用 x_3,x_4 来写出其他的 x 和目标函数 $c^{\mathrm{T}}x$，就得到了字典 3，而把各个变量都用 x_3,x_4 表示出来，因为既然要求 $x_3,x_4\geqslant 0$，字典 3 的最下一行就告诉我们，对于一切可行的 x，目标函数 $c^{\mathrm{T}}x$ 最多可以达到 6.

最后的字典里还包含了其他重要信息. 如果把约束条件里的向量 b 换成 $b+\varepsilon$，这里 ε 也是一个向量：$\varepsilon^{\mathrm{T}}=(\varepsilon_1,\varepsilon_2,\varepsilon_3)$. 如果这些 ε_i 都是很小的非负数，则目标函数 $c^{\mathrm{T}}x$ 的最大值将变成 $6+\frac{1}{3}\varepsilon_1+\frac{4}{3}\varepsilon_2$. 系数 $\frac{1}{3}$ 称为 "影子价格"(shadow price)，就是为了使 b 增加 1 个单位而愿意付出的价格.

3. 这个算法的功能

在运行单形算法时，重要的工作是计算这些字典. 为了算出字典 2，我们需要从字典 1 的第一个方程把 x_2 用 x_1,x_3 写出来，然后再以此代入其他方程中的 x_2. 后来，发明了单形算法的种种版本，都是利用矩阵 A 的构造的特殊的地方来减少计算量. 字典的数据通常放在所谓系数的表 (tableau) 中.

还有许多其他的实际的和理论的问题，其中之一是所谓 "枢纽"(pivot) 的选取问题. 所谓枢纽，就是要它从 0 开始变动的那个变量. 如果从可行区域 P 的顶点 O 开始，则看是选取 x_1 和 x_2 中的哪一个从 0 开始增加，而从 O 到最优的顶点 C 的路径可以分别是 O,E,D,C 或者 O,B,C. 还不知道有什么方法可以保证路径最短.

单形算法究竟需要多少步数，这个问题与著名的 Hirsch 猜想有关. 这个猜想就是：具有 m 个面的 n 维多胞体的直径 (即两个顶点间沿着棱的最短路径所包含的棱数的最大值) 最多是 $m-n$. 如果这个猜想为真，则意味着某个单形算法有一种版本运行完成的步数随着变量和约束的个数而线性地增长. 然而在 (Klee and MInty, 1972) 中给出了一个例子，以一个扰动的立方体 (具有 $m=2n$ 个面，直径为 n) 为

基础, 在其中, 如果这个单形算法想要选择枢纽变量, 使得当这个变量增长一个单位时, 目标函数能以最大速率增长, 则必须遍访所有 2^n 各顶点才能找到最优的枢纽变量. 事实上, 对于绝大多数决定性的选择枢纽变量的规则都能找到这样的例子, 使得步数随 n 指数增长.

幸运的是, 在实际问题中, 情况通常远比最坏的例子更好. 要解决一个具有 m 个约束的问题, 所需的步数典型地只是 $O(m)$. Khachian(1979) 通过分析所谓的椭球算法, 证明了线性规划问题可以用运行时间只是随 n 多项式增长的算法来解决. 这样, 线性规划远比 "整数线性规划"(其中变量 $x_1, \cdots, x_n$ 要求只取整数值) 容易, 对于后者, 还不知道有没有多项式运行时间的算法.

Karmarkar (1984) 率先开创了线性规划问题的 "内解法"(interior method), 这种解法就是在多胞体 P 的内部运动, 而不是在顶点间运动, 而有时能够比单形算法更快地解决大的 LP 问题. 现代的计算机软件两种方法兼用, 可以很容易地解决含有数以百万计的变量和约束的 LP 问题.

进一步阅读的文献

Dantzig G. 1963. *Linear Programming and Extensions*. Princeton. NJ: Princeton University Press.

Karmarkar N. 1984. A new polynomial-time algorithm for linear programming. *Combinatorica*, 4: 373-95.

Khachian L G. 1979. A polynomial algorithm in linear programming. *Soviet Mathematics Doklady*, 20: 191-94.

Klee V and Minty G. 1972. How good is the simplex algorithm? In *Inequality* Ⅲ, edited by Shisha O. New York: Academic Press, 16: 159-75.

孤 子
(Solitons)

见线性与非线性波以及孤子 [Ⅲ.49]

III.85 特殊函数
(Special Functions)

T. W. Körner

假如遇到过的函数只是多项式的商, 而又要求我们去对 $x > 0$ 解微分方程

$$f'(x) = \frac{1}{x}, \tag{1}$$

并有初始条件 $f(1) = 0$.

如果用 $f(x) = P(x)/Q(x)$ 去试, 这里 P, Q 是没有公因子的多项式, 则将有

$$x(Q(x)P'(x) - Q'(x)P(x)) = Q(x)^2.$$

比较双方系数将会得到 $Q(0) = P(0) = 0$. 这说明 P 与 Q 都可以用 x 整除, 而与 P, Q 没有公因子的假设矛盾. 所以, 只使用已知函数是不能解出方程 (1) 的. 然而, 微积分的基本定理[I.3 §5.5] 告诉我们, 方程 (1) 连同初始条件确实有解, 即

$$F(x) = \int_1^x \frac{1}{t}\mathrm{d}t.$$

进一步的研究还发现, 这个函数 F 有许多有用的性质. 例如作代换 $u = t/a$ 后就有

$$\begin{aligned} F(ab) &= \int_1^a \frac{1}{t}\mathrm{d}t + \int_a^{ab} \frac{1}{t}\mathrm{d}t = \int_1^a \frac{1}{t}\mathrm{d}t + \int_1^b \frac{1}{u}\mathrm{d}u \\ &= F(a) + F(b). \end{aligned}$$

再用反函数的微分公式, 就知道函数 F 的反函数 F^{-1} 是下面的微分方程

$$G'(x) = G(x)$$

以及初始条件 $G(0) = 1$ 的解. 所以, 给函数 F 一个名字 (对数函数), 并且把它纳入标准函数之内.

在更高的水平上, 分部积分说明, Gamma 函数[III.31](这是由欧拉[VI.19] 引入的)

$$\Gamma(x) = \int_0^\infty t^{x-1}\mathrm{e}^{-t}\mathrm{d}t$$

对一切 $x > 0$ 都有定义, 而且对所有 $x > 1$ 都具有下面的性质:

$$\Gamma(x) = (x-1)\Gamma(x-1),$$

所以对于一切整数 $n \geqslant 1, \Gamma(n) = (n-1)!$(因为 $\Gamma(1) = 1$). 由于 Gamma 函数与阶乘的关系, 我们可以期望它在数论和统计学中非常有用.

对于实际工作而言, 所谓 "特殊函数", 就是任意一种经过广泛研究, 证明用处很多的, 像是对数函数和 Gamma 函数那样的函数. 有些作者则在比较有限制的意义下使用特殊函数这个词, 意思是指 "出现在求解物理问题中的函数", 或者是指 "计算器上面没有的函数", 但是这些限制似乎没有什么用处.

尽管特殊函数具有明显的的一般性, 但在许多数学家心目中, 特殊函数总是和一大堆的特殊的思想和方法联系在一起的. 说真的, 总是和一些特定的书, 例如 Whittaker 和 Watson 的 *A Course of Modern Analysis* (这本书第一版是 1902 年, 可是到现在还卖得很火), 还有 Abramowitz 和 Stegun 的 *Handbook of Mathematical Functions* 这样的书. 这些联系可能不过是历史的偶然, 但是它又时常和另外一些短语相联系, 例如, "数学物理方程" "漂亮的公式" "十足的机敏" 等等. 现在从勒让德多项式 (Legendre polynomials) 这个特例来说明这个思想以及其他的一些思想 (下面一段涉及比较高深的数学, 而且绕过了一些较长的计算, 但是读者可以现在只略微浏览, 以后再细读).

假设要通过*拉普拉斯方程*[I.3 §5.4] $\Delta u = 0$ 的解来研究地球的引力势 ψ. 因为地球是一个稍微扁平的球形体, 不妨采用球坐标 (r, θ, φ), 再注意到地球对于其旋转轴是对称的, 可以假设 ψ 只依赖于 r 和 θ. 在这些假设下, 拉普拉斯方程形为

$$\sin\theta \frac{\partial}{\partial r}\left(r^2 \frac{\partial \psi}{\partial r}\right) + \frac{\partial}{\partial \theta}\left(\sin\theta \frac{\partial \psi}{\partial \theta}\right) = 0. \tag{2}$$

按照标准的分离变量法来求它的形如 $\psi(r,\theta) = R(r)\,\Theta(\theta)$ 的解. 稍经计算以后, 由 (2) 就可以得出

$$\frac{1}{R(r)}\frac{\mathrm{d}}{\mathrm{d}r}\left(r^2 R'(r)\right) = -\frac{1}{\sin\theta}\cdot\frac{1}{\Theta(\theta)}\frac{\mathrm{d}}{\mathrm{d}\theta}\left(\sin\theta\cdot\Theta'(\theta)\right). \tag{3}$$

因为方程一侧只依赖于 r, 而另一侧只依赖于 θ, 所以双方都等于某个常数 k. 从它的左侧得到

$$\frac{1}{R(r)}\frac{\mathrm{d}}{\mathrm{d}r}\left(r^2 R'(r)\right) = k,$$

当 $k = l(l+1)$ 时, 它有一个解 $R(r) = r^l$. 于是, 对于 $\Theta(\theta)$ 有相应的方程

$$\frac{1}{\sin\theta}\cdot\frac{1}{\Theta(\theta)}\frac{\mathrm{d}}{\mathrm{d}\theta}\left(\sin\theta\cdot\Theta'(\theta)\right) = -l(l+1). \tag{4}$$

现在作变量变换 $x = \cos\theta, y(x) = \Theta(\theta)$ 把 (4) 变成勒让德方程

$$(1-x^2)\,y''(x) - 2xy'(x) + l(l+1)\,y(x) = 0. \tag{5}$$

用常规的比较系数方法来求形如 $f(x) = \sum_{j=0}^{\infty} a_j x^j$ 的解, 就会发现, 除非 l 是一个整数, 当 x 趋近于 1(即 θ 趋近于 0, [也就是在北极附近]) 时, $f(x)$ 一定是无界的, 而这种无界的解在物理上是没有意义的. 然而, 如果 l 是一个正整数, 则会得到方程 (5) 一个 l 次的多项式解 (如果 l 是一个负整数, 也会得到同样的解). 事实上, 还可

以证明一个更强的结果: 如果 l 是一个正整数, 则勒让德方程 (5) 仅有一个满足条件 $y(1)=1$ 的 l 次多项式解, [用记号 $P_l(x)$ 来表示它], 并且称它为 l 次勒让德多项式. 回到原来的方程 (2), 我们知道地球有以下形状的引力势:

$$\psi(r,\theta)=\sum_{n=0}^{\infty}A_n\frac{P_n(\cos\theta)}{r^{n+1}}.$$

如果附带还要求当 $r\to\infty$ 时, 引力势还是有界的, 则上面的解是最一般的. 这一点对于物理学家是明显的, 而对于数学家则是可以证明的. 注意, 如果 r 很大, 则在上式中只有前面少数几项对最终的答案有看得出来的贡献.

有许多不同的方法可以得出勒让德多项式, 请读者自行验证下面所说的几个方法. 如果归纳地定义多项式 $Q_n(x)$ 如下: 令 $Q_0(x)=1, Q_1(x)=x$, 往下则用 "3 项递推公式":

$$(n+1)Q_{n+1}(x)-(2n+1)xQ_n(x)+nQ_{n-1}(x)=0$$

来计算其他 $Q_n(x)$, 则会得到 $Q_n(1)=1$, 而且 $Q_n(x)$ 是一个满足方程 (5)(在其中令 $l=n$) 的 n 次多项式, 这样就知道 $Q_n(x)$ 是 n 次勒让德多项式.

另外, 如果令 $v_n(x)=(x^2-1)^n$, 则

$$(x^2-1)v_n'(x)=2nxv(x),$$

用莱布尼兹法则把此式双方均微分 n 次, 就会发现 $v_n^{(n)}$ 也满足 $l=n$ 的勒让德方程 (5). [还要看一下 $v_n^{(n)}$ 是否满足 $P_n(1)=1$ 这样的条件]. 事实上, 若把 $v_n(x)=(x^2-1)^n$ 写成 $(x-1)^n(x+1)^n$, 用莱布尼兹公式微分 n 次, 就知道当 $x=1$ 时其结果只余下一项不为 0, 而有 $v_n^{(n)}(1)=2^nn!$. 把所有这些信息集中起来, 就得到勒让德多项式的 Rodriguez 公式:

$$P_n(x)=\frac{1}{2^nn!}v_n^{(n)}(x)=\frac{1}{2^nn!}\frac{\mathrm{d}}{\mathrm{d}x}(x^2-1)^n.$$

方程 (5) 连同条件 $y(1)=1$ 是斯图姆 (Jacques Charles François Sturm, 1803—1855, 法国数学家)-刘维尔[VI.39] 问题的一个例子. 令 $l=n$ 并且稍微改写一下, 就有方程

$$\frac{\mathrm{d}}{\mathrm{d}x}\left(\left(1-x^2\right)P_n'(x)\right)+n(n+1)P_n(x)=0. \tag{6}$$

如果 m 和 n 都是正整数, 然后利用 (6) 式并作分部积分, 就会得到

$$-n(n+1)\int_{-1}^{1}P_n(x)P_m(x)\,\mathrm{d}x$$

$$
\begin{aligned}
&= \int_{-1}^{1} \left(\frac{\mathrm{d}}{\mathrm{d}x} \left(\left(1-x^2\right) P_n'(x) \right) \right) P_m(x) \, \mathrm{d}x \\
&= \left[\left(1-x^2\right) P_n'(x) P_m(x) \right]_{-1}^{1} + \int_{-1}^{1} \left(1-x^2\right) P_n'(x) P_m'(x) \, \mathrm{d}x \\
&= \int_{-1}^{1} \left(1-x^2\right) P_n'(x) P_m'(x) \, \mathrm{d}x.
\end{aligned}
$$

由对称性, 就有

$$
m(m+1) \int_{-1}^{1} \left(1-x^2\right) P_n'(x) P_m'(x) \, \mathrm{d}x = n(n+1) \int_{-1}^{1} \left(1-x^2\right) P_n'(x) P_m'(x) \, \mathrm{d}x.
$$

如果 $m \neq n$, 就有

$$
\int_{-1}^{1} \left(1-x^2\right) P_n'(x) P_m'(x) \, \mathrm{d}x = 0. \tag{7}
$$

由 (7) 式给出的"正交关系"有许多重要的推论. 因为多项式 $P_r(x)$ 的次数恰好是 r, 我们知道任意的次数小于或等于 $n-1$ 的多项式 $Q(x)$ 必定可以写为

$$
Q(x) = \sum_{r=0}^{n-1} a_r P_r(x),
$$

所以

$$
\int_{-1}^{1} P_n(x) Q(x) \, \mathrm{d}x = \sum_{r=0}^{n-1} a_r \int_{-1}^{1} P_n(x) P_r(x) \, \mathrm{d}x = 0. \tag{8}
$$

这样, $P_n(x)$ 正交于所有次数较低的多项式.

现在假设 $P_n(x)$ 在区间 $[-1,1]$ 中改变符号的点是 $\alpha_1, \cdots, \alpha_m$. 这样, 若令

$$
Q(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_m),
$$

则 $P_n(x) Q(x)$①在 $[-1,1]$ 上不会再变号, 而有

$$
\int_{-1}^{1} P_n(x) Q(x) \, \mathrm{d}x \neq 0.
$$

而由 (8) 式可知 $Q(x)$ 的次数不会小于或等于 n : $m \geqslant n$. 但是, $P_n(x)$ 作为 n 次多项式恰好有 n 个零点, 所以 $P_n(x)$ 在区间 $[-1,1]$ 中改变符号的点的个数 $m \leqslant n$. 总之就有 $m=n$, 而 $P_n(x)$ 在区间 $[-1,1]$ 中恰好有 n 个实零点.

---

① 原书误为 $P(x)Q(x)$. —— 中译本注

高斯 [VI.26] 利用这些事实给出了强有力的数值积分的方法. 设 $x_1, x_2, \cdots, x_{n+1}$ 是区间 $[-1,1]$ 中的相异的点. 如果令

$$e_j(x) = \prod_{j\neq i} \frac{x - x_i}{x_j - x_i}, \quad 1 \leqslant j \leqslant n+1,$$

则 $e_j(x)$ 是一个 n 次多项式, 它在 x_j 处为 1, 而在 $x_i, i \neq j$ 处为 0. 这样, 如果 R 是次数至多为 n 的多项式, 则若令

$$S(x) = R(x_1) e_1(x) + R(x_2) e_2(x) + \cdots + R(x_{n+1}) e_{n+1}(x) - R(x),$$

即知它也是一个次数最多为 n 的多项式, 而且 $S(x_i) = 0, i = 1, 2, \cdots, n+1$. 所以 $S(x) \equiv 0$, 而有

$$R(x) = R(x_1) e_1(x) + R(x_2) e_2(x) + \cdots + R(x_{n+1}) e_{n+1}(x).$$

如果记 $a_j = \int_{-1}^{1} e_j(x)\,\mathrm{d}x$, 则对上式积分, 就有

$$\int_{-1}^{1} R(x)\,\mathrm{d}x = a_1 R(x_1) + a_2 R(x_2) + \cdots + a_{n+1} R(x_{n+1}).$$

既然已经对所有的次数至多为 n 的多项式证明了以上的等式, 我们当然希望对于其他的性态适当的函数 f, 确切的等式能够成为近似式

$$\int_{-1}^{1} f(x)\,\mathrm{d}x \approx a_1 f(x_1) + a_2 f(x_2) + \cdots + a_{n+1} f(x_{n+1}). \tag{9}$$

[前面定义 $e_j(x)$ 时所用的 x_i 都是任意的点, 而与勒让德多项式没有关系]. 高斯看到了如果取这些 $x_i, i = 1, 2, \cdots, n+1$ 就是第 $n+1$ 个勒让德多项式 $P_{n+1}(x)$ 在 $[-1,1]$ 中的 $n+1$ 个零点 (前面证明了 $P_{n+1}(x)$ 恰好在 $[-1,1]$ 中有 $n+1$ 个相异的实零点), 就可以得到很大的改进. 于是, 令 S①为任意次数最多为 $2n+1$ 的多项式, 则可以用第 $n+1$ 个勒让德多项式 $P_{n+1}(x)$ 去除它, 而得到

$$S(x) = Q(x) P_{n+1}(x) + R(x),$$

这里, 商 $Q(x)$ 由于 S 的次数最多为 $2n+1$, 所以是一个次数最多为 n 的多项式, 而余式 $R(x)$ 的次数不会超过 $P_{n+1}(x)$ 的次数, 所以也是次数最多为 n 的多项式. 因为勒让德多项式 $P_{n+1}(x)$ 正交于所有次数较低的多项式, 当然也包括 $Q(x)$, 就有

$$\int_{-1}^{1} S(x)\,\mathrm{d}x = \int_{-1}^{1} Q(x) P_{n+1}(x)\,\mathrm{d}x + \int_{-1}^{1} R(x)\,\mathrm{d}x = 0 + \sum_{j=1}^{n+1} a_j R(x_j)$$

①这里把原来用的 P 改成了 S, 目的是为了避免混淆.—— 中译本注

$$= \sum_{j=1}^{n+1} a_j (P_{n+1}(x_j) Q(x_j) + R(x_j)) = \sum_{j=1}^{n+1} a_j S(x_j),$$

这里 $x_j, j = 1, 2, \cdots, n+1$ 是勒让德多项式 $P_{n+1}(x)$ 的零点, 所以 $P_{n+1}(x_j) = 0$, 而由上面的除式又可任意得到 $S(x_j) = R(x_j)$.

这样又看到, 当按照高斯的建议把 x_j 选为勒让德多项式 $P_{n+1}(x)$ 的零点时, 近似的求积公式 (9) 对于任意的次数不高于 $2n+1$ 的多项式 $S(x)$ 又变成了精确的等式. 毫不令人奇怪, 这样的选择给出了极佳的数值估计积分的方法. 现在, "高斯求积法" 是在计算机上估计积分的两种主要方法之一.

我们再简短地提一下少数几个其他的特殊函数, 作为本文的结束.

考虑棣莫弗 (Abraham De Moivre, 1667—1754, 法国数学家) 公式

$$\cos n\theta + \mathrm{i} \sin n\theta = (\cos\theta + \mathrm{i} \sin\theta)^n.$$

由二项展开式, 有

$$\cos n\theta + \mathrm{i} \sin n\theta = \sum_{r=0}^{n} \binom{n}{r} \mathrm{i}^r \cos^{n-r}\theta \sin^r\theta.$$

取其实部, 可得

$$\cos n\theta = \sum_{r=0}^{[n/2]} \binom{n}{2r} (-1)^r \cos^{n-2r}\theta \sin^{2r}\theta.$$

因为 $\sin^2\theta = 1 - \cos^2\theta$, 有

$$\cos n\theta = \sum_{r=1}^{[n/2]} \binom{n}{2r} (-1)^r \cos^{n-2r}\theta \left(1 - \cos^2\theta\right)^r = T_n(\cos\theta),$$

这里的 T_n 是一个 n 次多项式, 称为切比雪夫 (Pafnuty Lvovich Chebyshev, 1821—1894, 俄罗斯数学家, 见 [VI.45]) 多项式. 切比雪夫多项式在数值分析中起重要作用.

下面一组函数要用无限和来考虑. 读者们要么认为下面的计算是可信的, 要么就自己去验证一下这些计算, 视自己的兴趣而定. 首先要看到

$$h(x) = \sum_{n=-\infty}^{\infty} \frac{1}{(x - n\pi)^2},$$

对于每一个实的 x, 只要它不是 π 的倍数, 都是有定义的. 还要注意, $h(x+\pi) = h(x)$, 还有 $h\left(\frac{\pi}{2} - x\right) = h\left(\frac{\pi}{2} + x\right)$. 令 $f(x) = h(x) - \csc^2(\pi x)$, 由于可以找到常

数 K_1 和 K_2 使得对于所有的 $0<x\leqslant\frac{1}{2}\pi$ 有

$$0<\sum_{n=1}^{\infty}\frac{1}{(x-n\pi)^2}<K_1,$$

以及

$$0<\csc^2 x-\frac{1}{x^2}<K_2,$$

由此得知, 存在一个常数 K 使得对于整个区间 $0<x<\pi$ 有 $|f(x)|<K$. 简单的计算表明

$$f(x)=\frac{1}{4}\left[f\left(\frac{1}{2}x\right)+f\left(\frac{1}{2}(x+\pi)\right)\right]. \tag{10}$$

使用 (10) 式一次, 可得 $|f(x)|<\frac{1}{2}K$, [使用 m 次可得 $|f(x)|<\left(\frac{1}{2}\right)^m K$, 所以有]$f(x)=0$. 这样可知对于所有不是 π 的整数倍的实数 x 有

$$\csc^2 x=\sum_{n=-\infty}^{\infty}\frac{1}{(x-n\pi)^2}.$$

如果要找出它在复平面上的类比, 就会被引到以下类型的函数:

$$F(z)=\sum_{n=-\infty}^{\infty}\sum_{m=-\infty}^{\infty}\frac{1}{(z-n-m\mathrm{i})^2}.$$

注意到实函数 $\csc^2 x$ 满足关系式 $\csc^2(x+\pi)=\csc^2 x$, 所以是以 π 为周期的周期函数, 则刚才的复函数 $F(z)$ 满足下面两个关系式:

$$F(z+1)=F(z),\quad F(z+\mathrm{i})=F(z),$$

所以是以 1 和 i 为周期的双周期函数. 这样的函数称为椭圆函数, 而且有一个和三角函数[III.92] 理论平行的理论.

函数 $E(x)=(2\pi)^{-1/2}\,\mathrm{e}^{-x^2/2}$ 称为高斯函数或正态函数. 它出现在概率理论和扩散过程的研究中 (见条目 [III.71 §5] 和 [IV.24]). 偏微分方程

$$\frac{\partial^2\phi}{\partial x^2}(x,t)=K\frac{\partial\phi}{\partial t}(x,t)$$

给出了扩散过程的一个合理的模型. 这里 x 表示距离, 而 t 表示时间. 很容易验证, 函数 $\phi(x,t)=\psi(x,t)=(Kt)^{-1/2}\,E(x(Kt)^{-1/2})$ 是这个方程的一个解. 对于不同的

t 值, 画出 $\psi(x,t)$ 作为 x 的函数的图像, 读者将会看到 ψ 可以看作是在 $t=0$ 时, $x=0$ 处的扰动在时刻 t 的响应. 对于给定的 x, 把函数 $\psi(x,t)$ 看作时间 t 的函数, 读者会看到 "一个位于原点的扰动在 x 点的效应, 要在量级为 $x^{1/2}$ 的时间以后, 才是可觉察的." 活细胞依赖于扩散过程, 而上面的结果 (正确地) 暗示了这个过程在长距离上是很缓慢的. 很可能这为活细胞的大小设置了一个限度, 所以大的机体必定是多细胞的.

统计学家经常使用所谓误差函数:

$$\operatorname{erf}(x)=\frac{2}{\pi^{1/2}}\int_0^x \exp\left(-t^2\right)\mathrm{d}t.$$

刘维尔[VI.39] 有一个著名的定理说: $\operatorname{erf}(x)$ 不可能表示为初等函数 (如多项式的商、三角函数和指数函数[III.25]) 的复合.

在本文中只能看少数几个特殊函数的少数几个性质, 但是虽然这个样本很小, 却已经足以显示, 研究一个或一类特定的函数, 而不是研究一般的函数, 会引起多么有趣的数学.

III.86　谱

(The Spectrum)

G. R. Allan

在向量空间[I.3 §2.3] 上的线性映射 [I.3 §4.2] 即线性算子的理论中, 本征值与本征向量[I.3 §4.3] 的概念起了重要作用. 回忆一下, 若 V 是一个 ($\mathbf{R}$ 上或 $\mathbf{C}$ 上的) 向量空间, 而 $T:V\to V$ 是一个线性映射, 则 T 的所谓本征向量就是 V 中的一个非零向量 e, 使得有一个标量 λ 存在, 满足 $T(e)=\lambda e$; 而 λ 就称为相应于本征向量 e 的本征值. 若 V 是有限维空间, 则本征值就是 T 的特征多项式 $\chi(t)=\det(tI-T)$ 的根. 因为每一个非零的复多项式都有根存在 (这叫做代数的基本定理[V.13]), 所以有限维的复向量空间的每一个线性算子至少有一个 [复的] 本征值存在. 如果取标量域为 $\mathbf{R}$, 则并非所有线性算子都有 [实] 本征向量存在 (例如考虑 $\mathbf{R}^2$ 上的旋转即知).

出现在分析中的线性算子通常是作用在无限维空间 (见 [III.50]) 上的. 我们考虑作用在一个复巴拿赫空间[III.62] 上的连续线性算子, 并在下面就简称它们为算子 (虽然并不是所有的作用在一个无限维巴拿赫空间上的线性算子都是连续的). 现在要指出, 对于无限维的 X, 并非所有这类算子都有本征值.

例 1　令 X 为由实轴上的闭区间 $[0,1]$ 上的所有连续复值函数所成的巴拿赫空间 $C[0,1]$, 它的向量空间结构就是 "自然的" 结构 (例如, 对于 $f,g\in X$, $f+g$ 就

定义为对于每一个 $t, (f+g)(t) = f(t)+g(t)$, 而范数就定义为上确界范数, 即所有 $|f(t)|$ 中的最大值).

现在令 u 为 $[0,1]$ 上的一个连续复值函数. 可以在 $C[0,1]$ 上作一个与之相关的乘法算子 [(或称乘子运算)]M_u 如下: 给定一个函数 f, 令 $M_u(f)$ 就是映 $t \in [0,1]$ 到 $u(t)f(t)$ 的函数. 映射 M_u 很清楚是线性连续的. 我们会看到 M_u 是否有本征值, 取决于函数 u 的选择. 我们来看两个简单的例子.

(i) 令 u 为常值函数 $u(t) \equiv k$, 显然 M_u 有唯一的一个本征值 k, 而每一个非零的函数 $f \in X$ 都是它的本征向量.

(ii) 令对于所有的 $t \in [0,1], u(t) = t$. 设复数 λ 是 M_u 的一个本征值. 这时, 有某个不恒为 0 的 $f \in C[0,1]$ 使得 $u(t)f(t) = \lambda f(t)$, 也就是对于一切的 $t \in [0,1]$ 有 $(t-\lambda)f(t) = 0$. 但这时对于所有的 $t \neq \lambda$ 均有 $f(t) = 0$. 因为 f 是连续的, 所以 $f(t) \equiv 0$ 而与假设相矛盾. 因此对于这样选择的 u, M_u 没有本征值.

令 X 为一个复巴拿赫空间, 而 T 是其上的一个算子. T 是可逆的, 当且仅当存在 X 上的算子 S 使得 $ST = TS = I$(这里 ST 是 T 与 S 的复合, 而 I 是 X 上的恒等算子). 可以证明, T 为可逆的当且仅当 T 既是单射 (即仅对于 $x = 0$ 有 $T(x) = 0$), 又是满射 (即 $T(X) = X$). 这件事情的证明里, 下面这一部分不是简单的代数运算、那就是证明当 T 既为单射又为满射时, T^{-1} 也是连续算子. 恰好是在 $T - \lambda I$ 不是单射时, λ 是 T 的一个本征值.

如果 V 是一个有限维空间, 则单射算子 $T: V \to V$ 必同时为满射算子, 从而 T 是可逆的. 如果 X 是无限维的, 这样的蕴涵关系就不再成立了.

例 2 令 H 为由所有满足以下条件的复数序列 $(\xi_n)_{n\geqslant 1}$ 所成的空间: $\sum_{n\geqslant 1} |\xi_n|^2 < \infty$. 这个空间记作 l^2, 它是一个希尔伯特空间[III.37]. 令 S 为 "右平移算子", 其定义为 $S(\xi_1, \xi_2, \xi_3, \cdots) = (0, \xi_1, \xi_2, \cdots)$, 则 S 是单射但不是满射. 考虑 "反向平移"(或称左平移)S^*, 其定义为 $S^*(\xi_1, \xi_2, \xi_3, \cdots) = (\xi_2, \xi_3, \cdots)$, 它就是一个满射, 但不是单射.

把这个例子记在心里, 我们就来给出下面的定义.

定义 3 令 X 为一个复巴拿赫空间, 而 T 是其上的一个算子. T 的谱 $\mathrm{Sp}(T)$(或记为 $\sigma(T)$) 就是使得 $T - \lambda I$ 不可逆的复数 λ 的集合.

以下的说明应该都是很清楚的事情.

(i) 若 X 是有限维空间, 则 $\mathrm{Sp}(T)$ 就是 T 的本征值的集合.

(ii) 若 X 是一般空间, 则 $\mathrm{Sp}(T)$ 既包括 T 的本征值的集合, 还可能大一点 (例如在例 2 中, 0 就不是 S 的本征值, 但是 0 确实在 S 的谱中).

很容易证明谱总是 $\mathbb{C}$ 的有界闭子集合 (即为紧集合[III.9]). 有一件相当深刻的事实就是: 谱绝不是空集合, 就是总有某个 λ 存在, 使得 $T - \lambda I$ 不是可逆的. 这个

定理的证明是对算子值解析函数 $\lambda\mapsto(\lambda I-T)^{-1}$ 应用刘维尔定理[I.3 §5.6], 这个函数对于不属于 T 的谱的 λ 有定义.

例 1(续) 我们已经见到, 并不是所有的乘法算子都有本征值. 然而, 它们却有容易描述的谱. 令 M_u 是这样一个算子, 而 S 为函数 $u(t)$ 的值域. 令 $\mu=u(t_0)$ 是这个函数的一个值, [即 S 的一点], 考虑算子 $M_u-\mu I$. 给定 $C[0,1]$ 中的一个函数 f, 则 $(M_u-\mu I)f$ 在 t_0 之值是 $u(t_0)f(t_0)-\mu f(t_0)=0$. 由此可见 $M_u-\mu I$ 不是满射 (例如 $M_u-\mu I$ 的值域就不包含任何一个非零的常值函数). 所以, μ 属于 M_u 的谱. 这样, 函数 $u(t)$ 的值域 S 完全包含在 M_u 的谱内. 实际上, S 和这个谱是相同的集合.

我们很容易推广这个例子来证明, 如果 K 是平面 $\mathbf{C}$ 的任意紧集合, 则一定存在一个线性算子 T 以 K 为谱. 令 X 为定义在 K 上的连续复值函数的空间, 则对任意的 $z\in K$, 令 $u(z)=z$, 而 T 是乘法算子 M_u, 原来它是对 $K=[0,1]$ 来定义的.

对于算子理论的许多侧面, 谱都处于一个中心位置. 我们要简短地提一下关于希尔伯特空间的谱的一个结果, 称为谱定理 (它有许多变体).

令 H 是具有内积 $\langle x,y\rangle$ 的希尔伯特空间. 如果对于 H 中的连续线性算子 T, 以及 H 的所有元 x 和 y, 都有 $\langle Tx,y\rangle=\langle x,Ty\rangle$, 就称 T 为一个厄尔米特算子.

例 4 (i) 若 H 是有限维的, 则 H 上的线性算子 S 为厄尔米特算子当且仅当 S 对于 H 的某一个规范正交基底, 从而也就是对于 H 的一切规范正交基底是一个厄尔米特矩阵 (即一个适合条件 $A=\bar{A}^{\mathrm{T}}$ 的矩阵)A.

(ii) 在希尔伯特空间 $L_2[0,1]$ 上, 令 M_u 是乘以连续复值函数 $u(t)$ 的算子 (从表面上看, 这个例子和例 1 是一样的, 但是现在是把 M_u 作用到 $L_2[0,1]$ 上, 而不是作用到 $C[0,1]$ 上). 这时, 当且仅当 u 仅取实值时, M_u 为厄尔米特算子.

如果 H 是有限维的, 而 T 是其上的厄尔米特算子, 则 H 具有一个由 T 的本征向量构成的规范正交基底 (即 "对角线基底"). 与此等价, $T=\sum_{j=1}^{k}\lambda_jP_j$, 这里 $\{\lambda_1,\cdots,\lambda_k\}$ 是 T 的相异的本征值, 而 P_j 是 H 到本征空间 $E_j\equiv\{x\in H:Tx=\lambda_jx\}$ 上的正交投影.

如果 H 是无限维的, 而 T 是其上的厄尔米特算子, 则一般说来 H 并不一定具有本征向量所成的基底. 但是, 很重要的是, $T=\sum_{j=1}^{k}\lambda_jP_j$, 这个表示确实可以推广为一种表示: $T=\int\lambda\mathrm{d}P$, 这是一种定义在 T 的谱上的 "投影值测度" 的积分.

[在有限维和无限维之间]有一种中间的情况, 即所谓紧厄尔米特算子的情况, "紧性" 作为一种很强的连续性, 在应用上有很大的重要性. 这里的技巧比一般情况

要简单得多, 只涉及无限求和, 而不涉及积分. 在 Young(1988) 中, 可以找到很有可读性的介绍.

进一步阅读的文献

Young N. 1988. *An Introduction to Hilbert Space*. Cambridge: Cambridge University Press.

III.87 球 面 调 和 (Spherical Harmonics)

傅里叶分析[III.27]的起点是这样一个观察: 很广阔的一类以 2π 为周期的周期函数都可以分解成三角函数[III.92]$\sin n\theta$ 和 $\cos n\theta$ 的无穷线性组合, 也就是可以写成形如 $\sum_{n=-\infty}^{\infty} a_n \mathrm{e}^{in\theta}$ 的和.

一种有用的思想就是把定义在实数直线 $\mathbf{R}$ 上的周期函数 f 看作一个等价的定义在复平面上的单位圆周 T 上的函数 F. T 上的典型的点可以写成 $\mathrm{e}^{\mathrm{i}\theta}$, 而定义这个等价的函数 F 的方式, 就是定义 $f(\theta) = F\left(\mathrm{e}^{\mathrm{i}\theta}\right)$([这个定义首先是适用于 θ 的区间 $[0, 2\pi]$ 上的], 但是注意到如果对 θ 增加 2π, 则因 $\mathrm{e}^{\mathrm{i}\theta} = \mathrm{e}^{\mathrm{i}(\theta+2\pi)}$, 所以 $F\left(\mathrm{e}^{\mathrm{i}\theta}\right)$ 不会改变, 而因为规定是以 2π 为周期的周期函数, 所以 $f(\theta)$ 也不改变. [这样, 上面的定义对于 $\theta \in \mathbf{R}$ 仍然有效]).

如果 $f(\theta) = \sum_{n=-\infty}^{\infty} a_n \mathrm{e}^{in\theta}$, 用 z 来代表 $\mathrm{e}^{\mathrm{i}\theta}$, 则等价的函数 F 可以写成 $F(z) = \sum_{n=-\infty}^{\infty} a_n z^n$, 所以如果用考虑 T 上的函数来代替考虑 $\mathbf{R}$ 上的周期函数, 则傅里叶分析就是把 $\mathbf{R}$ 上的函数分解为 z^n 的无穷线性组合, 这里 n 是任意的整数 (正、负整数和 0).

函数 z^n 有什么特殊之处? 答案是: 它们是 T 的特征标, 就是说它们是仅有的定义在 T 上的非零连续函数 ϕ, 并且对 T 上的任意的 z 和 w 都满足关系式 $\phi(z+w) = \phi(z)\phi(w)$.

现在设想 F 不是定义在 T 上而是定义在 $\mathbf{R}^3$ 的单位球面 S^2(即定义于一个 2 维集合, 即满足 $x^2+y^2+z^2=1$ 的点 (x, y, z) 的集合) 上. 更一般地说, 对于定义在 S^{d-1}(即满足 $x_1^2+\cdots+x_d^2=1$ 的点 $(x_1, \cdots, x_d)$ 的集合 [而 $d>2$]) 上的函数 F 又可以说些什么呢? 有没有自然的方法, 至少是对于一些很好的函数把这样一个 F 按这些函数分解呢? 就是说有没有一个好方法把傅里叶分析推广到高维球面上呢?

S^2 和 S^1(即 T) 有一个重要的而且一开始就令人沮丧的区别. 定义 T 是一些

复数的集合, 而不是平面 $\mathbf{R}^2$ 的一些点的集合, 这样做是看中了 T 成为一个群. 与之对照的是, 球面 S^2 没有这样一个有用的群结构 (为什么这样? 请参看条目四元数, 八元数和赋范除法代数[III.76], 就可以得到一点线索), 所以我们不能谈论特征标. 这一点使得这时什么才是 "很好的函数" 也不太明显了, 而我们正是想把 F 分解为这种函数的.

但是, 还可以沿另外一种途径来解释为什么三角函数会自然出现, 而这个途径完全不涉及复数. 可以把 S^1 的典型的点写为 $(x,y), x^2+y^2=1$, 也可以等价地写为 $(\cos\theta, \sin\theta)$, 这里的 θ 是实数. 这样, 如果想避免复数的话, 基本的函数就是 $\cos n\theta$ 和 $\sin n\theta$, 但是它们也可以用 x 和 y 来表示. 例如, $\cos\theta$ 和 $\sin\theta$ 分别就是 x 和 y, 而 $\cos 2\theta = \cos^2\theta - \sin^2\theta = x^2 - y^2$, 等等 (注意, 因为 $x^2+y^2=1$, 所以, $x^2-y^2=2x^2-1=1-2y^2$). 一般情况下, $\cos n\theta$ 和 $\sin n\theta$ 总可以写成 $\cos\theta$ 和 $\sin\theta$ 的多项式, 所以, 基本的函数可以看成是某些多项式在单位圆周上的限制.

那么, 是哪些多项式呢? 结果是, 它们是调和的、齐次的. 一个调和的多项式 $p(x,y)$ 就是满足拉普拉斯方程[I.3 §5.4]$\Delta p=0$ 的多项式, 这里 Δp 表示

$$\frac{\partial^2 p}{\partial x^2}+\frac{\partial^2 p}{\partial y^2}.$$

例如, 如果 $p=x^2-y^2$, 则 $\dfrac{\partial^2 p}{\partial x^2}=2, \dfrac{\partial^2 p}{\partial y^2}=-2$, 所以 x^2-y^2 如我们所希望的, 是一个调和多项式. 因为拉普拉斯算子是一个线性算子, 所以调和多项式构成一个向量空间. 一个 n 次齐次多项式就是每一项的总次数都是 n 的多项式, 或者等价地说就是这样一个多项式 $p(x,y)$, 使得对于任意的常数 λ 都有 $p(\lambda x, \lambda y)=\lambda^n p(x,y)$. 例如 x^3-3xy^2 就是一个 3 次齐次多项式 (而且也是调和多项式). n 次齐次调和多项式构成所有调和多项式的向量空间的子空间. 当 $n=0$ 时, 其维数为 1, $n>0$ 时, 维数为 2($n>0$ 时, 这个空间就是所有形如 $A\cos n\theta + B\sin n\theta$ 的函数的空间, 多项式 x^3-3xy^2 例如就是 $\cos 3\theta$).

调和多项式的概念很容易推广到高维情况. 例如在 3 维情况, 调和多项式就是一个满足

$$\frac{\partial^2 p}{\partial x^2}+\frac{\partial^2 p}{\partial y^2}+\frac{\partial^2 p}{\partial z^2}=0$$

的多项式 $p(x,y,z)$. 一个 n 阶 d 维的球面调和, 就是一个 d 个变量的 n 次齐次的调和多项式在 $d-1$ 维的球面 S^{d-1} 上面的限制.

下面就是球面调和的一些性质, 正是这些性质使它们特别有用, 而且是圆周上的三角多项式的很接近的类比. 固定维数 d, 并用记号 $d\mu$ 表示单位球面 $S=S^{d-1}$ 上的哈尔测度. 这句话的基本意思就是说, 如果 $f: S\to\mathbf{R}$ 是一个可积函数, 则 $\int_S f\mathrm{d}\mu$ 表示它的平均值. [这些性质就是]:

(i) 正交性. 如果 p 和 q 都是 d 维的球面调和, 但次数不同, 则 $\int_S pq\mathrm{d}\mu=0$.

(ii) 完备性. 每一个属于 $L^2(S,\mu)$ 的函数 $f:S\to\mathbf{R}$(就是说 $\int_S|f(x)|^2\mathrm{d}\mu$ 存在而且有限的实值函数 f) 都可以写成 $\sum_{n=0}^{\infty}H_n$(它在 $L^2(S,\mu)$ 中收敛), 这里 H_n 是 n 次球面调和.

(iii) 分解的有限维性质. 对于每一个 d 和 n, n 阶的 d 为球面调和构成一个有限维向量空间.

从这三个基本性质就容易导出: $L^2(S,\mu)$ 有一个由球面调和构成的规范正交基底[III.37]. 为什么球面调和很自然? 为什么它们很有用? 这两个问题各有许多答案. 下面对这两个问题各给出一个答案.

可以推广作用在 $\mathbf{R}^n$ 上的函数的拉普拉斯算子 Δ, 使之作用于定义在任意黎曼流形[I.3 §6.10]M 上的函数. 这个推广记作 Δ_M, 称为 M 上的拉普拉斯–贝尔特拉米 (Eugenio Beltrami, 1835–1900, 意大利数学家) 算子, 它的性态会给出关于 M 的几何学的许多信息. 特别是拉普拉斯–贝尔特拉米算子可以定义在球面 S^{d-1} 上, 这时通常就称它为贝尔特拉米算子. 可以证明, 球面调和就是贝尔特拉米算子的本征向量[I.3 §4.3]. 更准确地说, 一个维数为 d、阶数为 n 的球面调和, 就是贝尔特拉米算子的对应于本征值 $-n(n+d-2)$ 的本征向量 (注意, $\cos n\theta$ 的 2 阶导数为 $-n^2\cos n\theta$ 恰好说明它是 $d=2$ 时的本征函数), 这就给出球面调和另一个更加自然但不那么初等的定义. 这个定义与拉普拉斯算子为自伴算子这个事实结合起来, 就能解释球面调和的许多这样性质 (请参看条目线性算子及其性质[III.50 §3], 那里对这个说明作了一些展开).

傅里叶分析之所以这样重要, 有一个理由在于许多重要的线性算子当作用于一个函数的傅里叶变换时就对角化了, 因而特别易于理解. 例如, 设 f 是一个光滑的周期函数, 而把它写成 $\sum_{n\in\mathbf{Z}}a_n\mathrm{e}^{in\theta}$, 则其 "导数" 为 $\sum_{n\in\mathbf{Z}}na_n\mathrm{e}^{in\theta}$[(但是这里的导数是指 $-\mathrm{i}\frac{\mathrm{d}}{\mathrm{d}\theta}$, 在涉及傅里叶变换、量子力学等对偶性起重要作用的地方, 人们总是这样做的)][①]. 所以, 如果用 $\widehat{f(n)}$ 和 $\widehat{f'(n)}$ 分别表示$f(\theta)$ 和 $-\mathrm{i}\frac{\mathrm{d}}{\mathrm{d}\theta}f(\theta)$ 的第 n 个傅里叶系数, 则有 $\widehat{f'(n)}=n\widehat{f(n)}$, 它告诉我们, 为了作出 $-\mathrm{i}\frac{\mathrm{d}}{\mathrm{d}\theta}f(\theta)$, 只需把 f 的傅里叶系数用函数 $g(n)=n$ 逐点相乘即可, 这是求解微分方程的一个很有用的技巧.

正如前面已经提到的那样, 球面调和是拉普拉斯算子的本征函数, 但是它们也能把好几个其他的线性算子也对角化. 球面拉东 (Johann Karl August Radon, 1887–

① 原书这里明显有疏漏, 所以作了修改.—— 中译本注

1956, 奥地利数学家) 变换是一个好例子. 这个变换的定义是: $f: S^{d-1} \to \mathbf{R}$ 的球面拉东变换 $\mathbf{R}f$ 是另一个由 S^{d-1} 到 $\mathbf{R}$ 的函数, 它在 x 处的值等于 f 在所有正交于 x 的点 y 的集合上的平均值. 它与比较普通的拉东变换有密切的关系, 通常的拉东变换把定义在平面上的函数变成它在直线上的平均值; 求拉东变换之逆对于医学图像处理如 CT 和 NMR 是很重要的. 可以证明, 球面调和就是球面拉东变换的本征函数. 更一般地说, 任意形为 $Tf(x) = \int_S w(x \cdot y) f(y) \, \mathrm{d}\mu(y)$ 的变换 (其中 w 是一个适当的函数 (或广义函数)) 都可以用球面调和来对角化. 与一个给定的球面调和相关的本征值可以用 Funk-Hecke 公式来计算.

球面调和给出了一种把*切比雪夫多项式和勒让德多项式*[III.85] 联系起来的方法, 并且说明二者都是很自然的概念. 切比雪夫多项式就是 x 的那些同时维数为 2 的调和多项式, 即它们是两个变量的齐次调和多项式在 S^1 上的限制. 例如, 因为对于单位圆周上所有的点 (x,y) 有 $x^2+y^2=1$, 前面讨论过的函数 x^3-3xy^2 在 S^1 上就等于 $4x^3-3x$, 所以 $4x^3-3x$ 就是一个切比雪夫多项式. 勒让德多项式则是 x 的那样一些多项式, 它们等于维数为 3 的球面调和在 S^2 上的限制. 例如, 令 $p(x,y,z)=2x^2-y^2-z^2$, 则 $\Delta p=0$, 而且在 S^2 上, 因为 $x^2+y^2+z^2=1$, 处处有 $p(x,y,z)=3x^2-1$, 所以 $3x^2-1$ 是一个勒让德多项式.

也可以证明它们就是按通常方式定义的切比雪夫多项式和勒让德多项式, 下面是这个证明的一个概述. 这些多项式通常都定义为一个多项式序列, 而在此序列中, 每一个次数的多项式各有一个, 通常是通过正交关系来定义的. 因为不同次数的球面调和都是互相正交的, 所以上面描述的多项式也满足某些正交关系. 当把这些正交关系算出来以后, 就会发现它们就是定义切比雪夫多项式和勒让德多项式的关系.

III.88 辛 流 形
(Symplectic Manifolds)

Gabriel P. Paternain

辛几何就是统领着经典物理学的几何学, 而且更为一般地说, 在帮助我们理解群在流形上的作用上起了重要的作用. 它与黎曼几何和复几何共有某些特性, 而在一类特殊的流形, 即凯勒 (Kähler) 流形上, 这三种几何统一起来了.

1. 辛线性代数

正如*黎曼几何*[I.3 §6.10] 是基于*欧几里得几何*[I.3 §6.2] 一样, 辛几何是基于所谓线性辛空间 $(\mathbf{R}^{2n}, \omega_0)$ 的几何学的.

给定平面 $\mathbf{R}^2$ 中的两个向量 $v=(q,p)$ 和 $v'=(q',p')$, 由 v 和 v' 所张的平行四边形的有符号的面积由下式给出:

$$\omega_0(v,v')=\det\begin{pmatrix} q' & q \\ p' & p \end{pmatrix}=pq'-qp'.$$

它也可以用一个矩阵 J 和内积表示为 $\omega_0(v,v')=v'\cdot Jv$, 其中 J 是一个 2×2 矩阵

$$J=\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

如果一个线性变换 $A:\mathbf{R}^2\to\mathbf{R}^2$ 能够保持面积和定向不变, 则对一切 v 和 v', 有 $\omega_0(Av,Av')=\omega_0(v,v')$.

辛几何研究如上面这样的有符号面积的量度, 也研究保持面积和定向的变换, 但是它可以用于一般的 $2n$ 维空间, 而不只是平面.

如果把 $\mathbf{R}^{2n}$ 分裂成为 $\mathbf{R}^n\times\mathbf{R}^n$, 则任意的 $\mathbf{R}^{2n}$ 向量 v 都可以写为 $v=(q,p)$, 而 q 和 p 分别属于 $\mathbf{R}^n$. 这时, 标准辛形式 $\omega_0:\mathbf{R}^{2n}\times\mathbf{R}^{2n}\to\mathbf{R}$ 是由下式定义的:

$$\omega_0(v,v')=p\cdot q'-q\cdot p'.$$

这里 "·" 表示 $\mathbf{R}^n$ 中通常的内积. 在几何上, $\omega_0(v,v')$ 可以解释为 v 和 v' 在 q_ip_i 平面上的投影所张的平行四边形的有符号面积之和 $\left[\sum_i(p_iq_i'-q_ip_i')\right]$, 也可以用矩阵写为

$$\omega_0(v,v')=v'\cdot Jv, \tag{1}$$

其中 J 是一个 $2n\times 2n$ 矩阵

$$J=\begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}, \tag{2}$$

而 I 是 $n\times n$ 单位矩阵. 一个保持两个向量 $v,v'\in\mathbf{R}^{2n}$ 的积 $\omega_0(v,v')$ 不变的线性映射 $A:\mathbf{R}^{2n}\to\mathbf{R}^{2n}$(即有 $\omega_0(Av,Av')=\omega_0(v,v')$) 称为线性辛变换; 或者换一个等价的说法, A 适合条件 $A^{\mathrm{T}}JA=J$ 时为一个辛矩阵, 这里 A^{T} 是 A 的转置矩阵. 线性辛变换之于辛几何, 犹如刚体运动之于欧几里得几何. $(\mathbf{R}^{2n},\omega_0)$ 的线性辛变换的集合是一个经典的李群[III.48 §1], 记作 $\mathrm{Sp}(2n)$. 可以证明, 辛矩阵 $A\in\mathrm{Sp}(2n)$ 的行列式[III.15] 为 1, 所以它也保持面积. 然而, 当 $n\geqslant 2$ 时, 其逆不一定成立. 例如当 $n=2$ 时, 线性映射

$$(q_1,q_2,p_1,p_2)\mapsto(aq_1,q_2/a,ap_1,p_2/a),$$

当 $a \neq 0$ 时, 行列式为 1, 但是只在 $a^2 = 1$ 时, 才是线性辛变换.

标准辛形式有三个值得注意的性质. 首先, 它是双线性的: 当 v' 固定不变时, $\omega_0(v, v')$ 对于 v 是线性的, 反过来也一样. 其次, 它是反对称的, 就是对于一切 v 和 v', $\omega_0(v, v') = -\omega_0(v', v)$, 特别有 $\omega_0(v, v) = 0$. 最后它是非退化的, 就是对于任意的非 0 的 v, 必定存在非 0 的 v', 使得 $\omega_0(v, v') \neq 0$. 标准辛形式 ω_0 并不是仅有的具有这三个性质的形式. 然而可以证明, 任意具有这三个性质的形式, 在适当的可逆的线性变量变换后都可以化成一个标准辛形式 (这是所谓达布定理的特殊情况). 这样, $(\mathbf{R}^{2n}, \omega_0)$ 在本质是是唯一的 $2n$ 维辛几何. 在奇数维空间中, 没有辛形式存在.

2. $(\mathbf{R}^{2n}, \omega_0)$ 的辛微分同胚

在欧几里得几何中, 所有的刚体运动都自动地是线性变换 (或仿射变换). 然而在辛几何中, 除线性辛变换外还有许多其他辛映射. $(\mathbf{R}^{2n}, \omega_0)$ 中的这些非线性辛映射是辛几何的主要研究主题之一.

令 $U \subset \mathbf{R}^{2n}$ 是一个开集合. 回忆一下: 一个映射 $\phi: U \to \mathbf{R}^{2n}$ 称为光滑的, 如果它具有各阶连续偏导数. 一个微分同胚则是一个具有光滑逆的光滑映射.

称一个非线性的映射 $\phi: U \to \mathbf{R}^{2n}$ 是一个辛映射, 如果对于每一个 $x \in U$, 由一阶偏导数所成的雅可比矩阵 $\phi'(x)$ 都是辛矩阵. 如果用非形式的说法, 一个辛映射就是一个在无穷小尺度上的性态犹如线性辛变换的映射. 因为线性辛变换的行列式为 1, 利用多元微积分可以断定, 辛映射 ϕ 总是局部保体积和局部可逆的. 粗略地说就是, 当 A 为 U 的充分小子集合时, $\phi: A \to \phi(A)$ 总是可逆的, 而且 $\phi(A)$ 与 A 体积相同. 然而, 当 $n \geqslant 2$ 时, 其逆不一定为真; 辛映射的类比保积映射的类受到的限制要多得多. Gromov 的非挤压定理 (见下文) 将说明二者的差别多么惊人.

辛映射早就在经典力学中以典则映射之名存在了. 在下一小节里将要解释这一点.

2.1 哈密顿方程

怎样生成非线性辛映射呢? 我们从探讨一个熟悉的例子开始. 考虑一个长为 l 而质量为 m 的单摆, 并令 $q(t)$ 表示它在时刻 t 与铅直方向所成的角. 它的运动方程是

$$\frac{\mathrm{d}^2 q}{\mathrm{d}t^2} + \frac{g}{l} \sin q = 0,$$

这里 g 是重力加速度. 如果定义动量 p 为 $p = ml^2 \dot{q}$, 就能把上面的二阶微分方程变换为相平面 $\mathbf{R}^2$ 中的一个一阶微分方程组:

$$\frac{\mathrm{d}}{\mathrm{d}t}(q, p) = X(q, p). \tag{3}$$

这里, 向量场 $X(q,p)$ 由下式给出: $X(q,p) = (p/ml^2, -mgl\sin q)$. 对于每一个 $(p(0),q(0)) \in \mathbf{R}^2$, 都有 (3) 的唯一解 $(p(t),q(t))$ 以 $(p(0),q(0))$ 为初值. 于是, 对于每一个固定的时刻 t 都有一个演化映射 (亦称流)$\phi_t : \mathbf{R}^2 \to \mathbf{R}^2$, 使得 $\phi_t(q(0),p(0)) = (q(t),p(t))$, 而且它有一个值得注意的性质, 即保持面积. 这一点可以从 X 为无散度看出, 所谓无散度就是

$$\frac{\partial}{\partial q}\frac{p}{ml^2} + \frac{\partial}{\partial p}(-mgl\sin q) = 0.$$

事实上, 对于每一个时刻 t, ϕ_t 都是 $(\mathbf{R}^2, \omega_0)$ 上的辛映射.

一般地说, 任意有限多个自由度的经典力学系统都可以类似地重新陈述, 使得演化映射 φ_t 都是辛映射, 而辛映射在这样的上下文中就称为典则映射. 爱尔兰数学家**哈密顿**[VI.37] 早在 170 多年前就已经一般地告诉我们怎么做了: 给定任意光滑函数 $H : \mathbf{R}^{2n} \to \mathbf{R}$(称为哈密顿函数), 一阶微分方程组

$$\frac{\mathrm{d}q_i}{\mathrm{d}t} = \frac{\partial H}{\partial p_i}, \quad i = 1, \cdots, n, \tag{4}$$

$$\frac{\mathrm{d}p_i}{\mathrm{d}t} = -\frac{\partial H}{\partial q_i}, \quad i = 1, \cdots, n \tag{5}$$

(在关于 H 的一定的温和的增长条件下, 但我们略去这些条件的讨论) 就会给出演化算子 $\phi_t : \mathbf{R}^{2n} \to \mathbf{R}^{2n}$, 使得它在每一个时刻 t 都是 $(\mathbf{R}^{2n}, \omega_0)$ 上的辛映射. 为了看出这件事与辛形式 ω_0 的关系, 可以把 (4), (5) 重写为

$$\frac{\mathrm{d}x}{\mathrm{d}t} = J\nabla H(x), \tag{6}$$

这里 $x = (q,p)$, ∇H 就是 H 的通常的梯度, J 则是矩阵 (2). 从 (6), (1) 和 ω_0 的反对称性不难证明, ϕ_t 对于每一个时刻 t 都是一个微分同胚 (主要的技巧是计算 $\omega_0(\phi_t'(x)v, \phi_t'(x)v')$ 对于 t 的导数, 并证明它为 0).

我们已经指出了辛映射是保持体积的. 哈密顿系统之保持体积 (这个结果称为刘维尔定理) 这一点在 19 世纪吸引了相当大的注意, 而且是**遍历理论**[V.9] 的驱动力量, 这个理论正是研究保测度变换的回归性质的.

辛映射 (亦即典则变换) 在经典物理学中起了重要的作用, 因为它允许用比较简单、易于分析的等价系统代替一个复杂的系统.

2.2 Gromov 的非挤压定理

辛映射和保持体积的映射区别何在? 为了回答这个问题, 设在 $\mathbf{R}^{2n}$ 中有两个连通开集合 U 和 V, 而我们希望用一个辛映射把 U 嵌入到 V 中. 就是说, 希望找到一个辛映射 $\phi : U \to V$ 使得 ϕ 是由 U 到它的像 $\phi(U)$ 上的同胚. 我们知道这

样一个 ϕ 是保持体积的, 所以需要加一个限制, 即 U 的体积最多只能等于 V 的体积. 但是, 是否就这一个限制是起作用的? 考虑以原点为中心、R 为半径的开球体 $B(R)=\{x\in\mathbf{R}^{2n}:|x|<R\}$, 它显然有有限体积. 不难把它"辛嵌入"到无限体积的圆柱

$$C(r)=\left\{(q,p)\in\mathbf{R}^{2n}:q_1^2+q_2^2<r^2\right\}$$

中去而无论 R,r 如何取值. 事实上, 线性辛变换

$$(q,p)\mapsto(aq_1,aq_2,q_3,\cdots,q_n,p_1/a,p_2/a,p_3,\cdots,p_n),$$

只要 a 是充分小的正数就可以实现这个嵌入. 但是, 如果考虑另一个体积无限的圆柱

$$Z(r)=\left\{(q,p)\in\mathbf{R}^{2n}:q_1^2+p_1^2<r^2\right\}.$$

可以考虑用类似的线性映射 $(q,p)\mapsto(aq_1,q_2/a,q_3,\cdots,q_n,ap_1,p_2/a,p_3,\cdots,p_n)$ 来试一下. 这个映射是保持体积的, 因为它的行列式等于 1, 而对于小的 a, 它把 $B(R)$ 嵌入到 $Z(r)$ 中. 但是, 它只在 $a=1$ 时才是辛映射, 所以它只在 $R\leqslant r$ 时才会给出一个辛嵌入. 人们会去想, 当 $R>r$ 时, 仍然会有一个非线性的辛嵌入把 $B(R)$ 挤压到 $Z(r)$ 里去, 但是 Gromov① 在 1985 年以后的一个深刻的"非挤压定理"(non-squeezing theorem) 中证明了这是不可能的.

虽然有了 Gromov 的这个深刻的结果, 以及随之而来的其他结果, 我们对于 $\mathbf{R}^{2n}$ 中的集合如何互相嵌入仍然知之不多.

3. 辛流形

在条目*微分拓扑*[IV.7] 中已经知道, 一个 d 维流形是一个*拓扑空间*[III.90], 而且其每一点都有一个邻域同胚于欧几里得空间 $\mathbf{R}^d$ 的一个开集合. 我们可以把 $\mathbf{R}^d$ 看成是这个流形的局部模型, 意思就是, 它描述了流形在很小的距离尺度上看起来是什么样子. 我们还从那里知道了光滑流形就是"转移函数"为光滑时的那种流形. 这就是说, 如果 $\psi:U\to\mathbf{R}^d,\phi:V\to\mathbf{R}^d$ 是两个坐标区图, [而且, $U\cap V\neq\varnothing$], 则从 $\phi(U\cap V)$ 到 $\psi(U\cap V)$ 的转移函数 $\psi\circ\phi^{-1}$ 是一个光滑函数.

辛流形也是类似地定义的, 但是现在局部模型是线性辛空间 $(\mathbf{R}^{2n},\omega_0)$. 更准确地说, 辛流形就是一个 $2n$ 维流形, 它可以用坐标区图的定义域来覆盖, 而且转移函数是 $(\mathbf{R}^{2n},\omega_0)$ 上的辛微分同胚.

当然, $(\mathbf{R}^{2n},\omega_0)$ 的任意开集合都是辛流形. 环面 $\mathbf{T}^{2n}$ 是辛流形的另一个例子, 它是 $\mathbf{R}^{2n}$ 对于 $\mathbf{Z}^{2n}$ 的作用的商. 换句话说, $\mathbf{R}^{2n}$ 的两个点 x 与 y, 如果 $x-y$ 具

①Mikhail Leonidovich Gromov, 1943 年生于俄罗斯, 后入法国籍. 因为他在几何学中的"革命性的贡献"(这是评奖委员会的话, 其中就包含了辛几何以及这个非挤压定理) 获得了 2009 年阿贝尔奖.—— 中译本注

有整数坐标, 就认为它们是等价的. 辛流形的其他重要例子还包括**黎曼曲面**[III.79]、**复射影空间**[III.72] 和**余切丛**[IV.6 §5]. 然而, 给定一个紧流形, 要决定是否可以指定一族坐标区图, 使它成为辛流形, 还是一个范围很广的未解决的问题.

我们已经看到, 利用 $(\mathbf{R}^{2n}, \omega_0)$ 可以对 $\mathbf{R}^{2n}$ 的任意平行四边形指定一个 "面积" $\omega_0(v, v')$. 在一个辛流形 M 中, 类似地, 但是只是对于 $p \in M$ 处的无穷小平行四边形指定其面积 $\omega_p(v, v')$, 这样一个平行四边形的两个轴 v 和 v' 是两个无穷小向量 (准确一些说, 是切向量). 有一个唯一的方法这样做, 使得 M 的坐标区图彼此辛同胚. 用**微分形式**[III.16] 的语言来说, 映射 $p \mapsto \omega_p$ 是一个反对称的非退化 2 形式, 这样就能够用来计算 M 的非无穷小 2 维曲面区域 S 的 "面积" $\int_S \omega$. 可以证明, 对于充分小的封闭曲面 S, 这个积分为 0, 所以 ω 是一个闭形式. 事实上, 一个辛流形可以抽象地 (即不用坐标区图) 定义为一个具有封闭的反对称的非退化的 2 形式 ω 的光滑流形; 达布的一个经典的定理断定, 这个定义和利用坐标区图的比较具体的定义是等价的.

最后, 凯勒 (Erich Kähler, 1906—2000, 德国数学家) 流形是一类特殊的辛流形. 它们是同时为复流形的辛流形, 而且这两个结构自然地互相相容, 这个相容性条件是 (1) 的推广. 注意到, 如果把 $\mathbf{R}^{2n}$ 中的点 (q, p) 与 $\mathbf{C}^n$ 中的 $p + \mathrm{i}q$ 等同起来, 则 $\mathbf{R}^{2n} \to \mathbf{R}^{2n}$ 的线性变换 J 就变成了 $\mathbf{C}^n \to \mathbf{C}^n$ 的 "乘以 i" 的线性变换

$$J : (z_1, \cdots, z_n) \mapsto (\mathrm{i}z_1, \cdots, \mathrm{i}z_n).$$

这样, (1) 式就把 (由 ω_0 给出的) 辛结构和 (由 "乘以 i" 给出的) 复结构联系起来了. 一个复流形就是在小的距离尺度上看起来像是 $\mathbf{C}^n$ 的区域一样的流形, 而转移函数需要是**全纯的**[I.3 §5.6](说一个光滑映射 $f : \mathbf{C}^n \to \mathbf{C}^n$ 是全纯的, 就是说它的每一个坐标分量 $f_i(z_1, \cdots, z_n)$ 对每一个变量 z_k 都是全纯的). 在复流形上, 可以用 i 去乘切向量. 这就在每一点 $p \in M$ 给出了一个线性映射 J_p 且使得对 p 点的任意切向量 v 有 $J_p^2 v = -v$. 凯勒流形就是一个复流形 M, 而它还具有一个辛结构 ω(可以用来计算无穷小平行四边形的有向面积) 和一个黎曼度量 g(可以用来计算在每一点 $p \in M$ 出的两个切向量 v 和 v' 的内积 $g_p(v, v')$. 这两个结构由一个类似于 (1) 的关系式连接起来:

$$\omega_p(v, v') = g_p(v', J_p v).$$

凯勒流形的例子有复向量空间 $\mathbf{C}^n$、黎曼曲面和复射影空间 $\mathbf{PC}^n$.

可以如下面那样得出非凯勒流形的辛流形的例子来: 取 $\mathbf{R}^4$ 对于一个群的辛作用的商, 这个群看起来像是 $\mathbf{Z}^4$, 但又不是通常的 $\mathbf{Z}^4$. 群结构的改变表现为一个拓扑性质 (第一个贝蒂 (Betti) 数是奇数), 这就阻碍了商成为凯勒流形.

进一步阅读的文献

Arnold V I. 1989. *Mathematical Methods of Classical Mechanics*, 2nd edn. Graduate Texts in Mathematics, volume 60. New York: Springer.

McDuff D, and Salamon D. 1998. *Introduction to Symplectic Topology,* 2nd edn. Oxford Mathematical Monographs. Oxford: Clarendon Press/Oxford Univesity Press.

III.89 张 量 积 (Tensor Products)

令 U, V 和 W 是某个域上的向量空间[I.3 §2.3], 则从 $U \times V$ 到 W 的双线性映射就是服从以下规则的映射 ϕ:

$$\phi(\lambda u + \mu u', v) = \lambda\phi(u, v) + \mu\phi(u', v),$$

以及

$$\phi(u, \lambda v + \mu v') = \lambda\phi(u, v) + \mu\phi(u, v').$$

就是说, 它对于每一个变元分别都是线性的.

许多重要的映射, 例如内积[I.37], 都是双线性的. 两个向量空间 U 和 V 的张量积 $U \otimes V$ 则是一种方法, 使得能借以获取可能定义在 $U \times V$ 上的 "最一般的" 双线性映射. 为了能够理解这句话的意思, 让我们试着想象, 从 $U \times V$ 到 "最一般的" 向量空间 W 的 "最一般的" 双线性映射是怎么回事. 为此, 对这个双线性映射, 不再使用记号 $\phi(u, v)$, 而使用记号 $u \otimes v$, [这里 $u \in U, v \in V$ 代表这两个向量空间的一般元素, 也就是说, "$\otimes$" 现在代表从 $U \times V$ 到 W 的 "最一般的" 双线性映射: $u \otimes v : U \times V \to W$]. 因为这个双线性映射① 是 "最一般的", 所以关于它, 我们所知的限于由 [上面的规则所能够导出的一切知识], 就是只知道它具有双线性. 例如我们知道 $u \otimes v_1 + u \otimes v_2 = u \otimes (v_1 + v_2)$, [因为它就是上面的第一个规则]. 这个例子可能暗示 $U \otimes V$ 就是由这些形如 $u \otimes v$ 的元素构成的, 但是情况并不如此, 因为没有办法把 $u_1 \otimes v_1 + u_2 \otimes v_2$ 化简为 $u \otimes v$ 的形状 (这反映了一个事实, 即从 $U \times V$ 到 W 的双线性映射的值一般并不构成 W 的一个子空间).

[$U \otimes V$ 就是 "$\otimes$" 的值域], 它是形如 $u \otimes v$ 的元的线性组合, 而且附带了这样一个规则, 即如果两个这样的线性组合由双线性 (即按照上面的规则) 而不得不相等的话, 就把它们等同起来. 例如, $(u_1 + 2u_2) \otimes (v_1 - v_2)$ 就和下面的线性组合视为相同的:

$$u_1 \otimes v_1 + 2u_2 \otimes v_1 - u_1 \otimes v_2 - 2u_2 \otimes v_2.$$

①原书误为 "线性映射".—— 中译本注

这个思想有一种比较形式化的表述方法, 就是说 $U\otimes V$ 有一种万有性质 (universal property)(关于万有性质更多的例子, 可以参看条目几何和组合群论[IV.10], 也可参看条目范畴[III.8]). 这里讲的性质就是, 给定任意的从 $U\times V$ 到 W 的双线性映射 ϕ, 必有一个线性映射 $\alpha:U\otimes V\to W$, 使得对于任意的 $u\in U, v\in V$ 均有 $\phi(u,v)=\alpha(u\otimes v)$. 就是说每一个定义在 $U\times V$ 上的双线性映射, 都自然地与一个定义在 $U\otimes V$ 上的线性映射相联系 (这个线性映射把 $u\otimes v$ 等同于 $\phi(u,v)$, 张量积定义里讲的线性组合的等同性质保证了这里讲的等同性可以相容地拓展到 $u\otimes v$ 的线性组合上去).

如果 U 和 V 都是有限维向量空间, 而分别以 $u_1,\cdots,u_m$ 和 $v_1,\cdots,v_n$ 为基底, 不难证明, 这时 $u_i\otimes v_j$ 是 $U\otimes V$ 的基底. 张量积还有一些重要性质: 它们是可交换的和结合的, 就是说 $U\otimes V$ 与 $V\otimes U$ 自然地同构; $U\otimes(V\otimes W)$ 与 $(U\otimes V)\otimes W$ 自然地同构.

我们一直是在讨论向量空间的张量积, 但是这个定义很容易推广到其他代数结构上去, 只要双线性的概念对这种代数结构有意义就行, 例如模[III.81 §3] 和 C^*-代数[IV.15 §3] 都有张量积. 有时, 两个结构的张量积不是马上就可以设想到的. 例如, 令 $\mathbf{Z}_n$ 是整数 mod$n$ 的集合, 取 $\mathbf{Z}_n$ 和 $\mathbf{Q}$ 并且把它们都看成 $\mathbf{Z}$ 上的模. 很容易证明, 它们的张量积为零. 这反映了一个事实, 就是 $\mathbf{Z}_n\times\mathbf{Q}$ 上的所有双线性映射都是零映射.

张量积出现在许多数学背景下, 量子群[III.75] 就是一个好例子.

超越数

(Trancendental Numbers)

见无理数和超越数 [III.41]

III.90 拓扑空间

(Topological Spaces)

Ben Green

想要了解连续函数[I.3 §5.2] 的概念, 拓扑空间是最基本的数学背景.

请回想一下, 说一个函数 $f:\mathbf{R}\to\mathbf{R}$ 是连续的标准定义是什么意思. 设 $f(x)=y$. 只要当 x' 接近 x 时, $f(x')$ 就接近于 y, 则 f 在 x 处是连续的. 当然, 要使得这个概念在数学上是严格的, 就需要把 "接近" 这个概念弄精确. 我们可以说, 如果

$|f(x')-f(x)|<\varepsilon$, 而 ε 是一个很小的正数, 那么 $f(x')$ 就是接近于 y 的, 而我们也可以认为, 只要 $|x-x'|<\delta$, 而 δ 是另一个小的正常数, 则 x 是接近于 x' 的.

说 f 在 x 连续, 如果不论 ε 取的多么小, 总可以找到适当的 δ(当然允许 δ 依赖于 ε). 而如果 f 在实数直线的每一点 x 都连续, 就说 f 是连续的.

怎么才能把 $\mathbf{R}$ 换成另一个集合 X 从而推广这个概念呢? 只有当能够判定何时 X 中的 x 和 x' 两点为 "接近的", 现在的定义才有意义. 对于可能并不是很好地嵌入在欧几里得空间中的一般的集合, 如果不添加上附加的结构, 这是办不到的 (当加上了这个附加的结构时, 就有了度量空间[III.56] 的概念, 度量空间就不如拓扑空间那么广泛).

如果没有接近性的概念, 怎样定义连续性呢? 在开集合的概念里面可以找到答案. 说一个集合 $U\subset\mathbf{R}$ 是一个开集合, 就是说对 U 中任意点 x, 都有一个区间 (a,b) 既包含 x, 而又包含在 U 中.

下面是一个有趣的练习题, 就是要验证, 如果 $f:\mathbf{R}\to\mathbf{R}$ 是连续的, 而 U 又是一个开集合, 则 $f^{-1}(U)$ 也是一个开集合, 反过来, 如果对于每一个开集合 $U, f^{-1}(U)$ 都是开集合, 则 f 一定是连续的. 这样, 至少是对于从 $\mathbf{R}$ 到 $\mathbf{R}$ 的函数, 可以只用开集合的概念就能刻画连续性, 接近性的概念只是在定义开性时才会用到.

现在转到形式的定义. 一个拓扑空间就是一个集合 X, 其中指定了一族子集合 A(其中的元素称为 X 的开集合), 满足以下的公理:

- 空集合 $\varnothing$ 和整个 X 都是开集合.
- A 对于其任意多个元素的并是封闭的 (所以, 如果 $(U_i)_{i\in I}$ 是一族开集合, 则 $\bigcup_{i\in I}U_i$ 也是开集合).
- A 对于有限交也是封闭的 (所以, 如果 $U_1,\cdots,U_k$ 都是开集合, 则 $U_1\cap\cdots\cap U_k$ 也是开集合).

子集合族 A 就称为 X 是的一个拓扑. 很容易验证, $\mathbf{R}$ 上的通常的开集合满足上面的公理, 所以 $\mathbf{R}$ 利用了这些开集合而构成一个拓扑空间.

拓扑空间的一个子集合称为闭集合, 当且仅当它的余集合是一个开集合. 注意 "闭" 并不是 "非开", 例如在空间 $\mathbf{R}$ 中, 半开区间 $[0,1)$ 既不是开集合又不是闭集合, 但是空集合则既是开集合又是闭集合.

注意, 我们并没有要求开集合具有许多性质, 这就使得拓扑空间的概念成了一个很一般的概念. 实际上, 在许多场合, 这个概念太过于一般, 所以, 对拓扑空间概念再要求一些性质会是很方便的. 举例来说, 一个拓扑空间 X 称为豪斯道夫[VI.68] 空间, 如果对 X 中任意两个不同点 x_1 和 x_2, 都能找到不相交但是分别包含 x_1 和 x_2 的开集合 U_1 和 U_2. 豪斯道夫拓扑空间 ($\mathbf{R}$ 是其一个明显的例子) 有许多有用的性质, 而一般的拓扑空间可能并不具有.

在前面已经看到, 对于从 $\mathbf{R}$ 到 $\mathbf{R}$ 的函数, 连续性概念可以完全用开集合的概

念来表述, 这意味着也可以定义拓扑空间之间的函数的连续性. 设 X 和 Y 是两个拓扑空间, 而 $f : X \to Y$ 是它们之间的函数, 只需当 $U \subset Y$ 是 Y 的任意开集合时, $f^{-1}(U)$ 也是 X 中的开集合时, 定义 f 是连续的即可. 值得注意的是, 我们找到了一个不依赖于距离概念的连续性的定义.

一个具有连续逆的连续映射称为一个同胚. 如果两个拓扑空间 X 和 Y 之间存在一个同胚, 则从拓扑学的观点看来它们是等价的. 在拓扑学教材里我们常看见这样的话, 说拓扑学家无法区别一个汽车轮胎和一个有柄的茶杯, 因为其中的一个可以连续变形为另一个 (当然要想象它们都是用橡皮泥做的).

如果 X 是一个拓扑空间, 为了描述它的拓扑有一个很有用的方法, 就是给出 X 的拓扑之基. 所谓基就是 X 的拓扑 A 的一个子集合 $B \subset A$, 而每一个开集合 (即 A 的任意元素) 都是 B 中的某些元素之并. 例如在 $\mathbf{R}$ 上, 所有的开区间的集合 $\{(a,b) : a < b\}$ 就构成 $\mathbf{R}$ 的通常的拓扑的基, 而 $\mathbf{R}^2$ 的基则是所有开圆盘的集合 $\{B_\delta(x) = \{y : |y-x| < \delta\}\}$.

现在给一些例子.

离散拓扑. 令 X 为任意集合, 并取 A 为 X 的所有子集合的集合. 证明拓扑空间的所有公理都得到满足是一件简单的事情.

欧几里得空间. 令 $X = \mathbf{R}^d$, 而 A 包含了所有在距离拓扑下的开集合. 就是说, $U \subseteq X$ 是开集合, 如果对于每一点 $u \in U$, 都存在一个 $\delta > 0$, 使得 $B_\delta(u)$ 包含于 U 中. 要证明拓扑空间的所有公理在这个情况下也满足, 只是稍微麻烦一点. 更一般地说, 对于任意度量空间, 开集合也可以类似定义, 使得它也成一个拓扑空间.

子空间拓扑. 若 X 是一个拓扑空间, 而 $S \subseteq X$, 也能把 S 做成一个拓扑空间. 我们宣布, S 中的开集合就是形如 $S \cap U$ 的子集合, 这里 $U \in A$ 是 X 中的一个开集合.

扎里斯基 (Zariski) 拓扑. 这是代数几何[IV.4] 里使用的拓扑, 它是通过给出闭集合来确定的 (再取余集合也就给出了开集合)—— 这些闭集合就是多项式方程组的零点轨迹. 例如在 $\mathbf{C}^2$ 中, 这些闭集合恰好就是以下形状的集合:

$$\{(z_1, z_2) : f_1(z_1, z_2) = f_2(z_1, z_2) = \cdots = f_k(z_1, z_2) = 0\},$$

这里 $f_1, \cdots, f_k$ 都是多项式. 证明这恰好给出一个拓扑, 可不是平凡不足道的事情. 困难在于证明闭集合的任意交仍然是闭集合 (这就等价于证明开集合的任意并都是开集合). 这是希尔伯特基定理的推论.

拓扑空间的概念是抽象性在数学中的力量的一个好例子. 定义是很简单的, 但是涵盖了很多种多样的许多情况, 然而它又有很丰富的内容, 使我们能给出许多有趣的定义, 而且完全在纯粹拓扑空间的世界里证明许多定理. 找一个熟悉的概念,

把它应用于 $\mathbf{R}^1$ 和 $\mathbf{R}^2$, 然后再试着在一般的拓扑空间的世界里找出它的类比, 这样做时常是很有趣的. 我们给出两个例子.

连通性. 粗略地说, 一个连通集合就是不能用明显的方法把它分开来的东西. 许多人会以为, 从 $\mathbf{R}^2$ 的许多合理的子集合的图形的清单里面, 容易分辨出哪些是连通的, 哪些是不连通的. 但是, 谁能够给出一个准确的数学定义, 使之适用于一切集合, 包括那些可能是很狂野的集合, 并且说出来它们是否连通的? 例如下面的空间

$$S = ((\mathbf{Q} \times \mathbf{R}) \cup (\mathbf{R} \times \mathbf{Q})) \setminus (\mathbf{Q} \times \mathbf{Q}).$$

它是由 $\mathbf{R}^2$ 的这样的点构成的: 这些点的两个坐标恰好有一个而且只有一个是有理数. 对这个 S 赋予子空间拓扑, 它是连通的吗? 结果是, 确实可以给出连通性的定义, 而且它不只适用于 $\mathbf{R}^2$, 而且适合于一切拓扑空间. 我们说一个拓扑空间是连通的, 如果它不能分裂成两个互相分离的非空的开集合之并. 请读者来判断, 上面的 S 是不是连通的.

紧性. 这是在整个数学中最重要的概念之一, 但是初看起来有点奇怪. 它来自试图把 (例如 $\mathbf{R}^2$ 中的) 有界闭集合的概念推广到一般的拓扑空间里去. 我们说 X 是紧的, 如果在任意覆盖 X 的开集合族 C(就是说 C 中的开集合之并是 X) 中, 能够选出一个有限的子族 $\{U_1, \cdots, U_k\} \subseteq C$ 仍然能够覆盖 X. 把这个定义特别用于具有通常的拓扑的 $\mathbf{R}^2$, 确实可以证明, 集合 $S \subseteq \mathbf{R}^2$(赋以子空间拓扑) 为紧, 当且仅当 S 是有界闭集合. 更多的信息可见条目紧性与紧化[III.9].

III.91　变　换
(Transforms)

T. W. Körner

如果有实数的有限序列 $a_0, a_1, \cdots, a_n$(简记为 a), 就可以得到多项式

$$P_a(t) = a_0 + a_1 t + \cdots + a_n t^n.$$

反之, 给出了一个次数为 $m \leqslant n$ 的多项式 Q, 又能得到唯一的实数序列 $b_0, b_1, \cdots, b_n$, 使

$$Q(t) = b_0 + b_1 t + \cdots + b_n t^n,$$

例如只要令 $b_k = Q^{(k)}(0)/k!$ 即可.

可以看到, 如果 $a_0, a_1, \cdots, a_n$ 和 $b_0, b_1, \cdots, b_n$ 都是有限序列, 而且当 $r > n/2$ 时, $a_r = b_r = 0$, 则

$$P_a(t) P_b(t) = P_{a*b}(t),$$

其中 $a*b=c$ 是一个序列 $c_0,c_1,\cdots,c_{2n}$, 而且

$$c_k=a_0b_k+a_1b_{k-1}+\cdots+a_kb_0,$$

在这些式子里, 如果 $i>n$, 就把 a_i,b_i 解释为 0. 这个序列称为 a 和 b 的卷积, [并且记作 $a*b$.]

为了看到这件事情的用处, 考虑投出两个骰子会发生什么事. 如果第一个骰子 a 给出数字 u 的概率是 a_u, 第二个骰子 b 显出 v 的概率是 b_v. 二者之和为 k 的概率就是上面给出的 c_k. 如果这两个骰子都是公正的, 则 a_u 和 b_u 当 $1\leqslant u\leqslant 6$ 时, 均为 1/6, 而当 $u>6$ 或 $u<1$ 时, 则为 0. 于是

$$P_c(t)=P_{a*b}(t)=P_a(t)P_b(t)=\left(\frac{1}{6}\left(t+t^2+\cdots+t^6\right)\right)^2.$$

但是这个多项式又可以重写为

$$\begin{aligned}&\frac{1}{36}\left(t(t+1)\left(t^4+t^2+1\right)\right)\left(t\left(t^3+1\right)\left(t^2+t+1\right)\right)\\=&\frac{1}{36}\left(t(t+1)\left(t^2+t+1\right)\right)\left(t\left(t^4+t^2+1\right)\left(t^3+1\right)\right)=P_A(t)P_B(t),\end{aligned}$$

这里 A,B 是两个新的序列: $A_1=A_4=1/6, A_2=A_3=2/6$, 而对其他的 $u, A_u=0$. 对于 B, 则有 $B_1=B_3=B_4=B_5=B_6=B_8=1/6$, 而对其他的 $v, B_v=0$. 这样, 如果再做两个公正的骰子 A 和 B, 但是 A 有两个面刻着 2, 两个面刻着 3, 一个面刻 1, 余下的面则刻 4; 至于 B, 则 5 个面上分别刻 1, 3, 4, 5, 6, 另一个面则刻 8, 则这样两个骰子投出总数为 k 的概率和用两个普通的公正的骰子 a 和 b 投出总数为 k 的概率是相同的. 通过分析多项式 $t+t^2+\cdots+t^6$ 的根不难证明, 对于公正的骰子的各个面, 非标准地刻上严格正的整数, 而且具有上面的性质, 这是唯一的方法.

这些一般的思想很容易推广到无穷序列上去. 如果 a 是序列 $a_0,a_1,\cdots$, 则可以定义一个 "无穷多项式"$(Ga)(t)$ 为 $\sum_{r=0}^{\infty}a_rt^r$, 暂时只是形式地对待这个和, 而不问它究竟具有什么意义. 和前面完全相似, 可以看到

$$(Ga)(t)(Gb)(t)=(G(a*b))(t),$$

这里 $c=a*b$ 是下面的无穷序列

$$c_k=a_0b_k+a_1b_{k-1}+\cdots+a_kb_0$$

(仍然称 c 为 a 和 b 的卷积).

有一个著名的问题, 问利用给定面值的钞票来找零, 有多少这方法能够找出 r 个单位的零钱 (例如, 用 1 元和 5 元的钞票, 有多少种方法找出 43 元零钱来). 如果用某一组面值的钞票有 a_r 种方法找出 r 元钱, 而用完全不同的另一组钞票则有 b_r 种方法, 不难看到, 如果两组面值的钞票都准许用, 则可以用 c_k 种方法找出 k 元钱来, 这里的 c_k 又是前面定义的数.

现在来看一下怎样把以上所述应用到一个简单情况, 即 [如果准许同时用 1 元钞票和 2 元钞票来找出 r 元零钱, 问一共有多少方法?] 设 a_r 是只用 1 元钞票付出 r 元的方法, [当然只有一种方法, 所以 $a_r = 1$, b_s 则是只用 2 元钞票付出 s 元的方法, 显然, 若 s 为奇数, 则 $b_s = 0$, 而若 $s = 2r$, 则 $b_{2r} = 1$]. 所以这时会得到

$$(Ga)(t) = \sum_{r=0}^{\infty} t^r = \frac{1}{1-t},$$

$$(Gb)(t) = \sum_{r=0}^{\infty} t^{2r} = \frac{1}{1-t^2}.$$

[如果允许同时用这两种钞票, 则如上所说, 应该有 c_r 种方法. 但是在这个简单情况, 可以比较简便地算出 c_r 来. 因为现在可以利用分项分式, 而有]

$$\begin{aligned}(Gc)(t) &= (G(a*b))(t) = (Ga)(t)(Gb)(t) = \frac{1}{(1-t)(1-t^2)} \\ &= \frac{1}{(1-t)^2(1+t)} = \frac{1}{2(1-t)^2} + \frac{1}{4(1+t)} + \frac{1}{4(1-t)} \\ &= \frac{1}{2}\sum_{r=0}^{\infty}(r+1)t^r + \frac{1}{4}\sum_{r=0}^{\infty}(-1)^r t^r + \frac{1}{4}\sum_{r=0}^{\infty} t^r \\ &= \sum_{r=0}^{\infty} \frac{2r+3+(-1)^r}{4} t^r.\end{aligned}$$

所以, 当 r 为奇数时, 可以有 $\frac{1}{2}(r+1)$ 种方法找出 r 元零钱来; 而当 r 为偶数时, 可以有 $\frac{1}{2}(r+2)$ 种方法找出 r 元零钱来. 在这个简单情况自然可以用直接计算得出 c_r, 但是上面指出的方法自动地可以适用于所有情况 (如果允许使用复根, 计算还会更简单).

我们就这样作出了一个"生成函数变换"(亦称 G 变换) 来把一个序列 $a_0, a_1, \cdots$ 变成一个 "形式泰勒级数"$\sum_{r=0}^{\infty} a_r t^r$. [说它是 "形式泰勒级数", 是因为我们没有为收敛性操心](这里的用语并非标准的用语, 绝大多数数学家就会简单地说它是生成函数[IV.18 §§2.4, 3]). 下面的两个例子说明我们怎样利用 G 变换来把关于序

列的问题重新陈述为关于泰勒级数的问题. 第一个问题是要找一个序列 u_n 使得 $u_0=0, u_1=1$, 而对一切 $n\geqslant 0$ 有

$$u_{n+2}-5u_{n+1}+6u_n=0.$$

注意到, 对于一切 $n\geqslant 0$ 有

$$u_{n+2}t^{n+2}-5u_{n+1}t^{n+2}+6u_nt^{n+2}=0,$$

对 n 求和, [并且记 $u=\{u_0,u_1,u_2,\cdots,u_n,\cdots\}$], 有

$$(Gu(t)-u_1t-u_0)-5(tGu(t)-u_0)+6t^2Gu(t)=0.$$

注意到 $u_0=0, u_1=1$, 重新排列上式, 即有

$$(6t^2-5t+1)(Gu)(t)=t.$$

这样, 用分项分式就可以得到

$$\begin{aligned} Gu(t)&=\frac{t}{6t^2-5t+1}=\frac{t}{(1-2t)(1-3t)}=\frac{-1}{1-2t}+\frac{1}{1-3t}\\ &=-\sum_{r=0}^{\infty}(2t)^r+\sum_{r=0}^{\infty}(3t)^r=\sum_{r=0}^{\infty}(3^r-2^r)t^r. \end{aligned}$$

由此可知 $u_r=3^r-2^r$.

下面再考虑一个几乎是不足道的例子, 就是要找一个序列 u_n 使得 $u_0=1$, 而对所有的 $n\geqslant 0$ 有

$$(n+1)u_{n+1}+u_n=0.$$

对每一个 t 有

$$(n+1)u_{n+1}t^n+u_nt^n=0.$$

[仍如上例一样定义 $u=u_0+u_1t+u_2t^2+\cdots$], 对所有的 n 求和, 并且假设通常的微分规则对于形式无穷和 $u=\sum\limits_{r=0}^{\infty}u_rt^r$ 仍然适用, 我们就有

$$(G_u)'(t)+(G_u)(t)=0.$$

这个微分方程给出 $(Gu)(t)=A\mathrm{e}^{-t}$, 而 A 为一个常数. 令 $t=0$, 就得到

$$1=u_0=(Gu)(0)=A\mathrm{e}^0=A.$$

这样,

$$(Gu)(t)=\mathrm{e}^{-t},$$

而 $u_r = (-1)^r / r!$.

可以把一个序列以及它的 G 变换的一些对应关系写下来:

$$\begin{aligned}(a_0, a_1, a_2, \cdots) &\leftrightarrow (Ga)(t),\\ (a_0+b_0, a_1+b_1, a_2+b_2, \cdots) &\leftrightarrow (Ga)(t) + (Gb)(t),\\ a*b &\leftrightarrow (Ga)(t)(Gb)(t),\\ (0, a_0, a_1, a_2, \cdots) &\leftrightarrow t(Ga)(t),\\ (a_1, 2a_2, 3a_3, \cdots) &\leftrightarrow (Ga)'(t).\end{aligned}$$

同样很重要的是能够从序列的 G 变换来重新恢复序列本身, 其方法之一是注意到

$$a_r = \frac{(G_a)^{(r)}(0)}{r!}.$$

可以如上面的例子那样, 把关于序列的问题转换为关于函数的问题, 反过来也行. 在教科书和考试题里面, 这样的转换的效果是使得问题简单化. 但是在实际生活里, 通常却会使问题变得更复杂. 然而, 偶尔也会交好运, 而正是这样的机遇使得变换成了数学家的武库里的有力武器.

迄今为止, 我们都是形式地处理 G 变换的. 然而, 如果我们想利用分析中的方法, 就得确知级数 $\sum\limits_{r=0}^{\infty} a_r t^r$ 是收敛的, 至少当 $|t|$ 很小时是收敛的. 如果 a_r 增加得不太快, 这个级数确实也是收敛的. 但是当我们想把我们的思想推广到"双向的"序列 $\{a_r\}$, 就是 r 可以取一切整数, 而不只是非负整数, 得到的是"双向的和" $\sum\limits_{r=-\infty}^{\infty} a_r t^r$, 这时就会遇到困难. 即令 $|t|$ 很小, $|t^r|$ 当 r 是绝对值很大的负数时会很大, 如果 $|t|$ 很大, 则 $|t^r|$ 当 r 是绝对值很大的正数时会很大. 在许多情况下, 我们能够希望的最好的结果也就只是 $\sum\limits_{r=-\infty}^{\infty} a_r t^r$ 当 $t = +1$ 和 $t = -1$ 时收敛. 但是讨论那些只在两个点上有定义的函数并不很有用. 这时, 一个挽救的方法是从实数域 $\mathbf{R}$ 转到复数域 $\mathbf{C}$.

如果有一个性态良好的复数序列 $\{a_r\}$, 其中 r 可以遍取一切整数 (而不只是非负整数) 值, 这时, 我们可以考虑和式 $\sum\limits_{r=-\infty}^{\infty} a_r z^r$, 其中的复数 z 在单位圆周上 (即 $|z| = 1$). 因为这样的 z 可以写为

$$z = \mathrm{e}^{\mathrm{i}\theta} = \cos\theta + \mathrm{i}\sin\theta$$

而 $\theta \in \mathbf{R}$, 所以更通用的说法是讨论 2π 周期函数 $\sum\limits_{r=-\infty}^{\infty} a_r \mathrm{e}^{\mathrm{i}r\theta}$. 这样就得到"傅里

叶级数变换"(这个用语又是不标准的)H, 其定义为

$$(Ha)(\theta)=\sum_{r=-\infty}^{\infty}a_r\mathrm{e}^{\mathrm{i}r\theta}.$$

H 变换把一个双向复数序列 $a=\{\cdots,a_{-2},a_{-1},a_0,a_1,a_2,\cdots\}$ 变为一个 2π 周期的复值函数 $f=Ha$. 但是, 历史上数学家却更喜欢反其道而行, 就是从 f 得出 a. 如果

$$f(\theta)=\sum_{r=-\infty}^{\infty}a_r\mathrm{e}^{\mathrm{i}r\theta},$$

则通过形式的论证可得

$$\begin{aligned}\frac{1}{2\pi}\int_{-\pi}^{\pi}f(\theta)\,\mathrm{e}^{-\mathrm{i}k\theta}\mathrm{d}\theta&=\frac{1}{2\pi}\int_{-\pi}^{\pi}\sum_{r=-\infty}^{\infty}a_r\mathrm{e}^{\mathrm{i}(r-k)\theta}\mathrm{d}\theta=\sum_{r=-\infty}^{\infty}\frac{a_r}{2\pi}\int_{-\pi}^{\pi}\mathrm{e}^{\mathrm{i}(r-k)\theta}\mathrm{d}\theta\\&=\sum_{r=-\infty}^{\infty}\frac{a_r}{2\pi}\int_{-\pi}^{\pi}[\cos(r-k)\theta+\mathrm{i}\sin(r-k)\theta]\,\mathrm{d}\theta=a_r.\end{aligned}$$

如果使用以下的记号

$$\hat{f}(k)=\frac{1}{2\pi}\int_{-\pi}^{\pi}f(\theta)\,\mathrm{e}^{-\mathrm{i}k\theta}\mathrm{d}\theta,$$

就会得到著名的傅里叶求和公式

$$f(\theta)=\sum_{r=-\infty}^{\infty}\hat{f}(r)\,\mathrm{e}^{\mathrm{i}r\theta}. \tag{1}$$

狄利克雷[VI.36] 在这个公式的自然的解释下 [也就是按照古典分析的解释] 证明了对于具有合理的良好性态的函数, 这个公式是成立的. 但是对于更加广泛的函数类, 这个公式适当的解释和证明还要等待长得多的时间 (见条目卡尔松定理[V.5]). 这个问题的许多方面至今仍有待解决.

值得提一下的是, 我们可以不作显式的计算就能从一个序列的 H 变换得到关于这个序列的定性的信息, 反过来也是一样. 例如, 如果 $\{a_r r^{m+3}\}$ 对于固定的非负整数 m 是一个有界序列, 则可以用逐项微分的方法来证明 Ha 是 m 次连续可微的, 而如果函数 f 是 m 次连续可微的, 又可以反复使用分部积分方法来证明 $\{r^m\hat{f}(r)\}$ 是一个有界序列.

设 f 表示一个馈入一个 "黑箱"(如电话系统) 的信号, 而且产生一个信号 Tf. 许多在物理和工程中重要的黑箱都具有一种 "无限线性", 即

$$T\left(\sum_{r=-\infty}^{\infty}c_r g_r\right)(\theta)=\sum_{r=-\infty}^{\infty}c_r T g_r(\theta),$$

这里 g_r 是形态良好的函数, 而 c_r 是常数. 许多这样的系统还有一个关键的性质, 即

$$Te_k(\theta) = \gamma_k e_k(\theta),$$

其中 γ_k 是某个常数, 而 $e_k(\theta)$ 表示函数 $\mathrm{e}^{\mathrm{i}k\theta}$. 换言之, 函数 $e_k(\theta)$ 是 T 的本征函数[I.3 §4.3]. 可以利用傅里叶求和公式得出

$$Tf(\theta) = \left(\sum_{r=-\infty}^{\infty} \hat{f}(r) Te_r\right)(\theta) = \sum_{r=-\infty}^{\infty} \gamma_r \hat{f}(r) e_r(\theta).$$

在这样的背景下, 把 f 看成是频率为 k 的简单信号的加权的和是有意义的.

数学家们总是喜欢看一看, 如果把和换成积分会得到什么. 在这个情况下得到的就是经典的傅里叶变换. 如果 F 是一个性态合理的良好的函数 $F:\mathbf{R}\to\mathbf{C}$, 则用下式来定义其傅里叶变换

$$\mathcal{F}F(\lambda) = \int_{-\infty}^{\infty} F(r)\,\mathrm{e}^{-\mathrm{i}\lambda s}\mathrm{d}s.$$

大学一二年级的分析课程的很大一部分, 典型地就是在这种变换及相应的主题的背景下教的. 利用这种分析课程, 不难得到以下的对应关系:

$$\begin{aligned}
F(t) &\leftrightarrow (\mathcal{F}F)(\lambda),\\
F(t)+G(t) &\leftrightarrow (\mathcal{F}F)(\lambda)+(\mathcal{F}G)(\lambda),\\
F*G(t) &\leftrightarrow (\mathcal{F}F)(\lambda)(\mathcal{F}G)(\lambda),\\
F(t+u) &\leftrightarrow \mathrm{e}^{-\mathrm{i}u\lambda}(\mathcal{F}F)(\lambda),\\
F'(t) &\leftrightarrow \mathrm{i}\lambda\mathcal{F}F(\lambda).
\end{aligned}$$

在这样的前后文里, 定义 F 和 G 的卷积为

$$F*G(t) = \int_{-\infty}^{\infty} F(t-s)\,G(s)\,\mathrm{d}s.$$

有一句话说, 傅里叶变换的重要性就在于它把卷积变成了乘积, 而卷积的重要性则在于它是被傅里叶变换变成了乘积的运算. 这句话是有道理的. 正如可以用 G 变换来解差分方程一样, 也可以用 F 变换来解出现在物理学和概率理论某些部分的重要类型的偏微分方程[I.3 §5.4]. 关于傅里叶变换, 更多的可见条目 [III.27].

把傅里叶求和公式 (1) 改变尺度, 可以得到以下的公式:

$$F(t) = \sum_{r=-\infty}^{\infty} \frac{1}{2\pi N}\int_{-N}^{N} F(s)\,\mathrm{e}^{-\mathrm{i}rs/N}\mathrm{d}s\cdot \mathrm{e}^{\mathrm{i}rt/N},$$

这里 $|t| < \pi N$. 如果令 $N \to \infty$, 则或多或少有点形式地得到

$$F(t) = \frac{1}{2\pi}\int_{-\infty}^{\infty} (\mathcal{F}F)(s)\,\mathrm{e}^{\mathrm{i}st}\mathrm{d}s.$$

它又可以给出一个了不起的公式

$$(\mathcal{F}\mathcal{F}F)(t) = 2\pi F(-t).$$

就和傅里叶求和公式一样, 也可以在很广泛的情况下证明这个傅里叶反演公式, 虽然时常要以用新奇的方式重新解释它为代价.

傅里叶反演公式虽然很美, 但应该注意, 在实际应用上和在理论上, 我们时常只需要知道, 如果 $\mathcal{F}F = \mathcal{F}G$, 则必有 $F = G$. 这个傅里叶变换的唯一性证明和应用起来时常都比较容易, 成立所需的条件也时常比反演公式更宽一些.

当谈到傅里叶求和是与 2π 周期函数相关联时, 我们说 $\hat{f}(r)$ 是量度了信号 f 中的频率为 $2\pi r$ 的部分. 类似地, $(\mathcal{F}F)(\lambda)$ 是量度了构成信号 f 的频率接近于 λ 的那些成分. 有一族不等式, 总称为海森堡不确定性原理, 本质上就是, 如果 $\mathcal{F}F$ 的绝大部分集中在很窄的频带里, 则信号 F 必定广为弥散. 这个事实对于我们运作信号的能力给了很强的限制, 而在量子理论中, 它起着中心的作用.

在本文开始处讲到了序列的变换, 而且看到处理单向的序列比处理双向的序列容易. 同样, 如果知道当 $t < 0$ 时 $F(t) = 0$, 则可以在更宽的函数类 $F : \mathbf{R} \to \mathbf{C}$ 中应用傅里叶变换. 更确切地说, 如果 F 是这样一个单向的函数, 而且增长不太快, 则可以计算它的拉普拉斯变换

$$(\mathcal{L}F)(x+\mathrm{i}y) = \int_{-\infty}^{\infty} F(s)\,\mathrm{e}^{-(x+\mathrm{i}y)s}\mathrm{d}s = \int_{0}^{\infty} F(s)\,\mathrm{e}^{-(x+\mathrm{i}y)s}\mathrm{d}s,$$

这里 x 和 y 都是实数, 而且 x 不太大. 如果采用更自然的记号

$$(\mathcal{L}F)(z) = \int_{0}^{\infty} F(s)\,\mathrm{e}^{-zs}\mathrm{d}s,$$

就会看到 $\mathcal{L}F$ 其实是全纯函数[I.3 §5.6](即复可微函数) 的加权平均, 而这一点就可以用来证明 $\mathcal{L}F$ 也是全纯函数. 拉普拉斯变换具有许多和傅里叶变换一样的性质, 而我们在对拉普拉斯变换进行操作时, 就可以应用这些性质和搜集起来的大量的关于全纯函数的性质. 数论中的许多最深刻的结果, 如素数定理[V.26], 绝大部分都可以通过灵巧地应用拉普拉斯变换而很容易获得.

我们所讨论的变换都属于同一族, 这一点可以从它们都把卷积化为乘积看出来. 变换的一般思想在几个不同方向发展, 这些方向一般地都是来自集中注意于“经典变换”的某一侧面, 而有意地忽略其他侧面.

这些新变换中最重要的之一是所谓盖尔范德 (Israil Moiseevich Gelfand, 1913–2009, 前苏联数学家) 变换, 它对于抽象的可交换巴拿赫代数给出了具体的表示. 这件事将在条目*算子代数*[IV.15 §3.1] 中讨论. 其他的积分变换则推广了傅里叶变换的积分定义, 建立起一个对应关系

$$F(t) \leftrightarrow \int_{-\infty}^{\infty} F(s)\, K(\lambda - s)\, \mathrm{d}s,$$

或者更一般的对应关系

$$F(t) \leftrightarrow \int_{-\infty}^{\infty} F(s)\, \kappa(s, \lambda)\, \mathrm{d}s.$$

另一个有趣的变换是拉东变换, 或称 X 射线变换. 这里只讨论 3 维情况, 而且只进行很不形式化的讨论. 设把一束射线沿方向 u 射入人体, 又设 f 是一个定义在 $\mathbf{R}^3$ 上的函数, 表示人体的各部分吸收了多少辐射. 我们能够量度的只是沿着给定的直线被吸收的辐射量. 可以把这个信息用一个 2 维图像来表示, 这个图像表示的就是沿着所有的方向为 u 的直线的吸收总量. 一般说来, 我们可以用 f 来得到一个新的函数

$$(\mathcal{R}f)(u, v) = \int_{-\infty}^{\infty} f(tu + v)\, \mathrm{d}t,$$

它告诉我们, 沿着一条方向为 u 的直线, 通过一个方向垂直于 u 的向量 v 吸收了多少辐射. 断层摄影术处理的就是怎样从 $\mathcal{R}f$ 来恢复 f.

因为变换的思想是在那么多不同方向上发展的, 所以给出一般的定义的任何企图都会失之过于宽泛而用处不大. 关于形形色色的变换, 我们能够说的最多也就是它们是经典的傅里叶变换的多少有点遥远的类比, 而发现这些变换的人觉得这种类比对他是有用的 (请参看以下各个条目: *傅里叶变换*[III.27]、*球面调和*[III.87]、*表示理论*[IV.9 §3] 和*小波及其应用*[VII.3]).

III.92 三 角 函 数
(Trigonometric Functions)

Ben Green

基本的三角函数 "sin" 和 "cos", 还有四个相关的函数 "tan" "cot" "sec" 和 "csc", 读者们, 大概多少都熟悉的它们的某种形式. 定义正弦函数 $\sin : \mathbf{R} \to [-1, 1]$ 有一种方式如下.

在几乎所有数学分支中, 都是用弧度来量度角度的. 弧度的定义以弧长为基础, 说图 1 中的角 $\angle AOB = \theta$ 弧度, 就是说, 在单位圆周上的圆弧 $\widehat{AB}$ 之长为 θ. 这个

定义当 $0 \leqslant \theta < 2\pi$ 时有意义. 然后, 定义 $\sin\theta$ 为线段 PB 之长, 这里 P 是自 B 所作的对于 OA 的垂线的垂足. 很重要的是, 对这个长度需要赋以正确的符号. 如果 $0 < \theta < \pi$, 就取正号, 而如果 $\pi < \theta < 2\pi$, 则取负号. 换句话说, $\sin\theta$ 就是点 B 的 y 坐标.

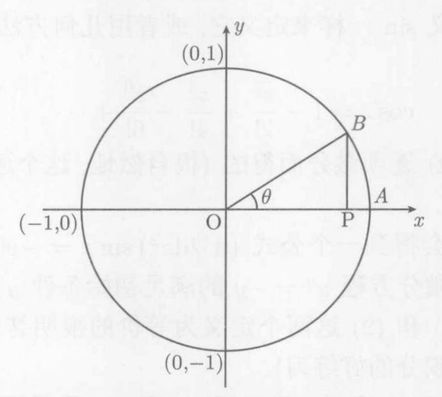


图 1 三角函数的几何解释

现在, 正弦函数还只是定义在区间 $[0, 2\pi)$ 上. 要在整个 $\mathbf{R}$ 上定义它, 只需坚持它是以 2π 为周期的周期函数即可 (就是说, 它应该对任意整数 n 都满足关系式

$$\sin\theta = \sin(2\pi n + \theta)).$$

关于正弦函数的定义还有一个问题. 所谓弧 $\widehat{AB}$ 的长度是什么意思? 要了解它, 真正令人满意的方法是用微积分. 单位圆周的方程是 $y = \sqrt{1-x^2}$, 至少是当 (x, y) 点位于第一象限时是如此 (否则的话, 在符号上就得小心). 曲线 $y = f(x)$ 的位于 $y = a$ 和 $y = b \quad (a \leqslant b)$ 之间的一段, 长为

$$S = \int_a^b \sqrt{1 + (\mathrm{d}x/\mathrm{d}y)^2}\,\mathrm{d}y$$

(这可以看成是一个定义, 虽然这个定义的动机来自图形). 对于圆周 $\sqrt{1+(\mathrm{d}x/\mathrm{d}y)^2} = 1/\sqrt{1-y^2}$, 因为单位圆周上点 $P = (x, \sin\theta)$ 和点 $A = (1, 0)$ 之间的一段弧长是 θ, 故有

$$\int_0^{\sin\theta} \frac{\mathrm{d}y}{\sqrt{1-y^2}} = \theta, \tag{1}$$

它适用于 $0 \leqslant \theta \leqslant \pi/2$.

和数学中许多最自然的概念一样, sin 可以用许多等价的方法来定义. 另一个定义 (它与上一个定义的等价性并不是一看就明白的) 是

$$\sin z = z - \frac{z^3}{3!} + \frac{z^5}{5!} - \frac{z^7}{7!} + \cdots. \tag{2}$$

这个无穷级数对所有实的 z 都收敛. 这样得到的定义, 有一点明显优于 (1), 即当 z 是任意复数时, 它也是有意义的 (这就是用 z 来代替字母 θ 的原因). 这就使得我们能够把 sin 推广成为 $\mathbf{C}$ 上的全纯函数[I.3 §5.6].

如果正弦函数是解析的, 那么它的导数是什么? 答案是: 它的导数是余弦函数 $\cos z$, 也可以完全像定义 sin 一样来定义它, 或者用几何方法, 或者用幂级数. 幂级数的定义是

$$\cos z = 1 - \frac{z^2}{2!} + \frac{z^4}{4!} - \frac{z^6}{6!} + \cdots, \tag{3}$$

这是从 sin 的级数式 (2) 逐项微分而得的 (很自然地, 这个运算需要适当地加以论证, 而这是可以做到的).

如果再次微分, 又会得到一个公式 $(\mathrm{d}^2/\mathrm{d}z^2)\sin z = -\sin z$. 事实上, 也可以定义 $\sin\colon \mathbf{R} \to [-1,1]$ 为微分方程 $y'' = -y$ 的满足初始条件 $y(0) = 0, y'(0) = 1$ 的唯一解. 这是一个证明 (1) 和 (2) 这两个定义为等价的很明智的方法 (用 (1) 式证明 $\sin'' = -\sin$, 是一个微积分的好练习).

最后, 幂级数展开式 (2) 和 (3) 显示了 sin 和 cos 最重要的方面, 就是它们与指数函数[III.25] 的关系. [指数函数的幂级数展开式是]

$$\mathrm{e}^z = 1 + z + \frac{z^2}{2!} + \frac{z^3}{3!} + \cdots,$$

与 (2), (3) 两式比较, 就得到著名的公式

$$\mathrm{e}^{\mathrm{i}\theta} = \cos\theta + \mathrm{i}\sin\theta.$$

指数函数 $\theta \mapsto \mathrm{e}^{in\theta}$ 是特征标, 就是说, 它可以看作由群 $\mathbf{R}/2\pi\mathbf{Z}$($\mathbf{R}$ 在 $\bmod 2\pi$ 的加法下所成的群) 到复平面 $\mathbf{C}$ 上的单位圆周 S^1(它在复数乘法下也成一个群) 的一个同态[I.3 §4.1]. 这使得它们成为作 $\mathbf{R}$ 上的 2π 周期函数的傅里叶分析[III.27] 的自然的对象. 因为 sin 和 cos 在 $\mathbf{R}$ 上都是实值函数, 所以我们不把 $\mathbf{R}$ 上的 2π 周期函数 $f(x)$ 写成指数函数的级数, 而写成下面的级数

$$a_0 + a_1\cos x + b_1\sin x + a_2\cos 2x + b_2\sin 2x + \cdots$$

这样作更加方便. 在相当宽松的条件下 (例如要求 f 充分光滑), 可以用下面这样的正交性关系

$$\frac{1}{\pi}\int_0^{2\pi} \cos nx\cos mx\mathrm{d}x = \begin{cases} 0, & \forall n, m \geqslant 0, n \neq m, \\ 1, & n = m, \end{cases}$$

还有

$$\frac{1}{\pi}\int_0^{2\pi} \cos nx\sin mx\mathrm{d}x = 0$$

来求出相应于 f 的 a_i, b_i.. 这样, 例如有

$$a_n = \frac{1}{\pi}\int_0^{2\pi} f(x)\cos nx\mathrm{d}x.$$

在许多装置如 CD 激光唱盘和手机里面, 最终都有这样的函数三角展开式.

最后再提一点作为本文的结束. 关于 sin, cos 还有其他四个相关的函数 (在本文中没有讨论它们) 的公式和涉及它们的积分纷纭万状, 犹如一个大花园. 正是这些公式使得三角函数成了经典的欧几里得几何的不可少的工具. 在这个背景下, 还有许多进一步的公式. 我们只举一个漂亮的例子: 内接于单位圆而且顶角为 A, B, C 的三角形, 面积为 $2\sin A\sin B\sin C$.

不可数集合

(Uncountable Sets)

见可数与不可数集合 [Ⅲ.11]

III.93 万有覆叠

(Universal Covers)

设 X 为一个**拓扑空间**[III.90]. X 中的环就定义为由闭区间 $[0,1]$ 到 X 的一个满足条件 $f(0) = f(1)$ 的连续映射 f. 环的一个连续族则是由 $[0,1]^2$(其中的元素记为 (t,s)) 到 X 的连续映射, [其中 t 表示这个族的参数, 而 s 表示 X 中的元] 使得对于所有的 $t\in[0,1]$ 均有 $F(t,0) = F(t,1)$. 这里的思想, 就是对于每一个 $t\in[0,1]$ 都可以用 $F(t,s)$ 作出一个环 $f_t(s) = F(t,s)$, 而得到 "连续依赖于 t 的一族环". 如果一个环可以连续变形而收缩为一点, 就说这个环是可收缩的. 比较形式一点地说, 就是由环的一个连续族 $F(t,s)$, 使得对于每一个 $s, F(0,s) = f(s)$, 而 $F(1,s)$ 则成为 X 中的一个固定点. 如果 X 中的所有的环都是可收缩的, 就说 X 是单连通的. 例如, 球面就是单连通的, 但是环面则不是, 因为有 "包围着环面转" 的但是不能在环面上收缩为一点的环 (因为每一个围着环面转的环, 无论如何变形, 也会绕环面同样多次).

给定任意的充分好的道路连通的空间 X(就是像流形那样的好空间 X, 而且具有以下的性质, 即其上的任意两点都可以用一条路径连接起来), 都能够定义一个与它关系密切的单连通空间 $\tilde{X}$ 如下: 在 X 中取任意的 "基点"x_0, 再作所有由 $[0,1]$ 到 X 的连续路径 f, 使之满足条件 $f(0) = x_0$(但是不要求 $f(1)$ 也是 x_0). 下一步

是规定这样两条路径 f 和 g 是等价的, 或者说是同伦的, 如果 $f(1)=g(1)$, 而且有一个连续的路径族, 从 f 连续地变形为 g, 且在变形过程中, 路径的起点一直是 $f(0)=g(0)=x_0$, 终点一直是 $f(1)=g(1)$. 也就是说, f 和 g 是同伦的, 如果存在一个由 $[0,1]^2$ 到 X 的连续映射, 使得对于一切 t 都有 $F(t,0)=f(0)=g(0)=x_0$, $F(t,1)=f(1)=g(1)$, 而且对于一切 s, $F(0,s)=f(s)$, $F(1,s)=g(s)$. 最后, 就定义 X 的万有覆叠 $\tilde{X}$ 为所有这些路径的同伦类所形成的空间, 也就是说, $\tilde{X}$ 是所有由 x_0 点出发的连续路径的空间关于同伦的*等价关系*[I.2 §2.3] 的商[I.3 §3.3].

现在我们来看在实际上是怎样做的. 前面已经说过, 环面不是单连通的, 那么, 怎么来作环面上的万有覆叠呢? 为了回答这个问题, 我们用一种比较人为的方法来看待环面: 固定环面上一点 x_0, 定义环面为所有以 x_0 为起点的而且位于环面上的连续路径的集合, 而如果两个这样的路径有共同的终点, 就认为它们是等价的. 如果我们这样做了, 则对于这样的路径, "我们所关心的" 只是它的终点的位置, 而终点的集合显然就是环面本身. 但是这还不是万有覆叠的定义. 在万有覆叠中, 我们关心的不只是路径的终点, 还有路径是如何达到其终点的. 例如, 如果路径是一个环, 则终点就是 x_0 本身, 那么我们关心的就是这条路径绕环面多少圈, 以及是怎样绕的.

环面可以定义为 $\mathbf{R}^2$ 对于下面的等价关系的商: $\mathbf{R}^2$ 上的两个点, 如果其坐标之差在 $\mathbf{Z}^2$ 中, 就认为是等价的. 这样, $\mathbf{R}^2$ 的任意点都被商映射映到环面上. 环面上的任意路径在下面的意义下被唯一地 "提升" 到 $\mathbf{R}^2$ 平面上: 在 $\mathbf{R}^2$ 上固定一个被映为环面上的 x_0 点的 u_0 点. 这时, 如果在环面上画出任意的以 x_0 点为起点的连续路径, 则在 $\mathbf{R}^2$ 上也就有一条以 u_0 为起点的路径, 而其上的点都被映到环面上的路径上的适当的点.

现在设在环面上有两条从 x_0 开始的路径, 而且都终于同样的 x_1 点. 这两条路径的 "提升" 都从 u_0 开始, 但是关于它们的终点, 我们所知的只有二者等价这一点, 并不知道这两个终点是否相同. 实际上, 如果第一条路径是环面上的可收缩的环, 而第二条路径则是绕环面一次的环, 它们的提升将终结于不同的点. 可以证明 (如果试着把结果可视化, 就会看到这个结果是很自然而且使人信服的), 这两个提升终结于同一点当且仅当环面上的两条路径为同伦的. 换句话说, 环面上的路径的同伦类与 $\mathbf{R}^2$ 上的点有一个一一对应. 这就表明, $\mathbf{R}^2$ 是环面的万有覆叠. 在一定意义下可以说, 从一个空间到它的万有覆叠的过渡把商运算 "展开" 了, 而我们正是用这个商运算从万有覆叠走到原来的空间的.

有一个富有成果的思考这个例子的方法, 就是考虑 $\mathbf{Z}^2$ 与 $\mathbf{R}^2$ 中的*群作用*[IV.9 §2] 的自然的联系: 这个作用把 $\mathbf{Z}^2$ 的点 (m,n) 和 $\mathbf{R}^2$ 中的平移 $(x,y)\mapsto(x+m,y+n)$ 联系起来, 而环面就可以看成是 $\mathbf{R}^2$①对于这个平移的商, 而环面的元素就是这个作

①原书在这里作 $\mathbf{Z}^2$, 似乎与下文矛盾.—— 中译本注

用的轨道, 而且赋以商拓扑 (这个轨道就是以下形状的集合 $\{(x+m, y+n) : (m, n) \in \mathbf{Z}^2\}$, 而商拓扑基本上就是说, 把认为直觉上互相接近的两个 $\mathbf{Z}^2$ 的平移看作是接近的), $\mathbf{Z}^2$ 在 $\mathbf{R}^2$ 上的作用是自由的和离散的. 意思是说 $\mathbf{Z}^2$ 中的任意非零的元素都把一个点的充分小的邻域移到这个邻域外面去了, 结果是每一个充分好的空间都是它的万有覆叠对于一个类似的群的商, 而这个群就是 X 的*基本群*[IV.6 §2].

万有覆叠顾名思义是一个万有性质. 粗略地说, 空间 X 的一个覆叠就是另一个空间 Y, 以及一个由 Y 到 X 的连续满射, 使得 X 中的一个小邻域的原像是 Y 的若干小邻域的离散并. 如果 U 是 X 的万有覆叠, 而 Y 是 X 的任意其他的覆叠, 则一定能以自然的方式把 U 变成 Y 的一个覆叠. 例如可以把一个无限长的圆柱面弯成环面的一个覆叠, 而圆柱面又可以用平面来覆叠. 这样, X 的所有连通的覆叠都是万有覆叠的商. 更进一步还有每一个覆叠又都是 X 的基本群的一个子群在万有覆叠上的作用的轨道空间. 看到这一点, 就能在 X 基本群的子群的共轭类与覆叠的等价类之间建立一个对应关系. 这样一个 "伽罗瓦对应" 在数学的其他地方也有类比, 其中最为经典的是域的扩张 (见条目*五次方程的不可解性*[V.21]).

万有覆叠的应用的一个例子可以在条目*几何和组合群论*[IV.10 §§7, 8] 中找到.

III.94 变 分 法
(Variational Methods)

Lawrence C. Evans

变分法一方面本身是一个理论, 另一方面又是研究某些类型的 (通常是高度非线性的) 常微分方程和偏微分方程的技巧的工具箱. 这种方程是在我们去寻找某些适当的 "能量" 函数的临界点时出现的, 它比起其他非线性问题要容易处理得多.

1. 临界点

让我们从一个在一年级微积分课程里就会出现的情况开始. 如果 $f = f(t)$ 是一个定义在实数直线 $\mathbf{R}$ 上的光滑函数, 而且在 t_0 点有一个局部极小 (或极大), 则 $(\mathrm{d}f/\mathrm{d}t)(t_0) = 0$.

变分法极大地推广了这个视点. 现在, 要考虑的基本的对象成了一个泛函 F, 它并不是作用在实数上, 而是作用在函数上, 或者更好是说, F 作用在某些可容许函数类上. 就是说, F 把函数 u 变成一个实数 $F(u)$. 如果 u_0 是 F 的一个极小化子 (minimizer)(即对于所有的可容许函数 u, 有 $F(u_0) \leqslant F(u)$), 我们可以期望 "F 的导数在 u_0 处为 0". 当然, 要把这个概念弄精确, 这件事可以预想得到是有点棘手的, 因为可容许函数的空间是无穷维的. 但是, 实际上这些所谓变分法正是在不超出标准的微积分的范围内, 对于极小化函数 u_0 的本性给出了深刻的洞察.

2. 一维问题

应用变分法技巧的最简单的情况涉及的是一元函数. 让我们来看一看为什么在这个情况下, 极小化子一定自动地满足某个常微分方程.

2.1　最短距离

我们来证明平面上连接两点的最短的路径是直线段, 并以此作为一个热身的问题. 这个问题的答案当然是显然的, 但是我们就此发展起来的方法, 却可以用于更有趣得多的问题.

于是, 设有平面上的两点 (a, A) 和 (b, B). 取可容许函数类为所有这样的光滑的实值函数 $u(x)$, 它们定义在某区间 $I = [a, b]$ 上, 而且适合 $u(a) = A, u(b) = B$①于是 $u = u(x)$ 是经过这两点的曲线, 它在这两点之间的一段长度为

$$F(u) = \int_I (1 + (u')^2)^{1/2} \mathrm{d}x, \tag{1}$$

这里 $u = u(x)$, 而一撇代表对 x 求导. 现在设有特定的可容许函数 u_0 使这个长度极小化. 我们想要导出 u_0 的图像是直线段, 做法是令在极小化子 u_0 处 "F 的导数为 0".

为了使得这个思想有意义, 选择任意一个定义在此区间 I 上而且在区间两端为 0 的光滑函数 w. 对于每一个 t 定义 $f(t) = F[u_0 + tw]$, 因为函数 $u_0 + tw$ 的图像仍然连接平面上的两点 (a, A) 和 (b, B), 而 u_0 又会给出最短长度, 可知 $f(t)$ 就是一个从 $\mathbf{R}$ 到 $\mathbf{R}$ 的普通的函数, 而在 $t = 0$ 出达到极小值. 所以 $(\mathrm{d}f/\mathrm{d}t)(0) = 0$. 但是可以通过在积分号下求导来显式地算出 $(\mathrm{d}f/\mathrm{d}t)(0)$, 然后再作分部积分, 这就会给出

$$\int_I \frac{u_0' w'}{\left(1 + (u_0')^2\right)^{1/2}} \mathrm{d}x = -\int_I \left(\frac{u_0'}{\left(1 + (u_0')^2\right)^{1/2}}\right)' w \mathrm{d}x.$$

这个恒等式对于一切具有上述性质的 w 都成立, 因此, 在整个区间 I 上有

$$\left(\frac{u_0'}{\left(1 + (u_0')^2\right)^{1/2}}\right)' = \frac{u_0''}{\left(1 + (u_0')^2\right)^{3/2}} = 0. \tag{2}$$

总结以上的讨论可知如果 u_0 的图像使得平面上所给的两点距离极小化, 则 u_0'' 恒为 0, 所以最短的路径一定是连接这两点的直线段. 这个结论不一定让人兴奋, 但

①这里记号稍有改动, 以免混淆.—— 中译本注

是即令是这样简单的例子也有有趣的特点. 变分法自动地把我们的注意力引向下面的表达式

$$\kappa=\frac{u''}{\left(1+(u')^2\right)^{3/2}},$$

而它就是 u 的图像的曲率: 极小化子 u_0 的图像曲率为 0.

2.2 推广: 欧拉–拉格朗日方程

事实证明, 我们用于前面的例子的方法是极为有力的, 而且能够极大地推广.

一个有用的推广是把上例中的长度泛函 (1) 换成更一般的形状如下的泛函:

$$F[u]=\int_I L(u',u,x)\,\mathrm{d}x, \tag{3}$$

这里的 $L=L(v,z,x)$ 是一个给定的函数, 有时称为拉格朗日函数. 这时 $F[u]$ 可以解释为定义在区间 I 上的已知函数 u 的 "能量"(或 "作用量").

下一步设一个特定的曲线 u_0 是 F 的极小化子, 而且满足某个固定的边值条件. 我们想要抽取出关于 u_0 的性态的信息, 而为此像前例一样进行. 像前面一样选一个函数 w, 定义 $f(t)=F[u_0+tw]$, 注意到 f 在 $t=0$ 处有极小值, 由此导出 $(\mathrm{d}f/\mathrm{d}t)(0)=0$. 和前面的计算一样, 我们来显式地计算这个导数:

$$\frac{\mathrm{d}f}{\mathrm{d}t}(0)=\int_I (L_v w'+L_z w)\,\mathrm{d}x=\int_I \left(-(L_v)'+L_z\right)w\mathrm{d}x,$$

这里, L_v 和 L_z 分别表示在 (u_0',u_0,x) 处取值的偏导数 $\partial L/\partial v, \partial L/\partial z$. 这个导数对所有满足已给条件的函数 w 均为 0. 所以, 在整个区间 I 上有

$$-\left(L_v\left(u_0',u_0,x\right)\right)'+L_z\left(u_0',u_0,x\right)=0. \tag{4}$$

这个关于 u_0 的非线性常微分方程称为欧拉–拉格朗日方程. 关键之点就在于泛函 F 的任意极小化子都必须是这个微分方程之解, 而在这个方程里就包含了重要的物理学与几何学信息.

例如, 取 $L(v,z,x)=\frac{1}{2}mv^2-W(z)$, 把它解释为一个沿实数直线 $\mathbf{R}$ 运动的质量为 m 的粒子的动能与位能 W 之差. 这时, 欧拉–拉格朗日方程就是

$$mu_0''=-W'(u_0).$$

这就是牛顿第二运动定律. 变分法给了我们关于这个基本的物理定律的漂亮的推导.

2.3 方程组

还可以进一步推广, 而令

$$F(u)=\int_I L(u',u,x)\,\mathrm{d}x, \tag{5}$$

这里取 u 为映区间 I 到 $\mathbf{R}^m$ 的向量值函数. 如果 u_0 是在适当的函数类中的极小化子, 则可以用类似于上面的讨论的方法来计算欧拉–拉格朗日方程. 这样, 对于每一个 $k\,(k=1,\cdots,m)$ 都会得到一个方程

$$-\left(L_{v^k}(u_0',u_0,x)\right)'+L_{z^k}(u_0',u_0,x)=0, \tag{6}$$

这里 L_{v^k} 和 L_{z^k} 分别是 L 对于向量 u' 和 u 的第 k 个分量的偏导数在 (u_0',u_0,x) 处所取的值. 这些方程构成了关于 $u_0=(u_0^1,\cdots,u_0^m)$ 的各个分量的耦合的常微分方程组.

举一个几何的例子, 令

$$L(v,z,x)=\left(\sum_{i,j=1}^{m}g_{ij}(z)\,v^iv^j\right)^{1/2}.$$

于是, $F[u]$ 就是曲线 u 在 g_{ij} 所决定的黎曼度量[I.3 §6.10] 下的长度. 如果 u_0 是具有常值单位速度的曲线, 经过一些计算就知道欧拉–拉格朗日方程组 (6) 可以写成

$$\left(u_0^k\right)''+\sum_{i,j=1}^{m}\Gamma_{ij}^k\left(u_0^i\right)'\left(u_0^j\right)'=0,\quad k=1,\cdots,m,$$

这里的 Γ_{ij}^k 是一些特定的表达式, 称为克里斯托费尔 (Elwin Bruno Christoffel, 1829–1900, 德国数学家) 记号, 可以用 g_{ij} 来表出. 这个常微分方程组的解称为测地线. 这样就导出了: 使长度极小化的曲线是测地线.

一个物理学的例子是 $L(v,z,x)=\frac{1}{2}m|v|^2-W(z)$, 对于它, 欧拉–拉格朗日方程组是

$$m\boldsymbol{u}_0''=-\nabla(\boldsymbol{u}_0).$$

这就是 $\mathbf{R}^m$ 中的质点在位能 W 的作用下运动的牛顿第二定律.

3. 高维问题

变分法也可以用于含有多元函数的表达式, 这时得到的欧拉–拉格朗日方程将是偏微分方程 (简记为 PDE).

3.1 最小面积

第一个例子是前面讲的最短曲线的推广. 对于这个问题, 已知的是平面上的一个区域 U, 其边缘是 ∂U, 还有一个定义在边缘上的实值函数 g. 然后就要找一个可容许函数类, 这个类中的函数 u 都是实值函数, 它们定义在 U 上, 而且在边缘上等于 g. 可以把 u 的图像想象为一个弯曲的曲面, 而且以 g 的图像 [(这个图像是定义在 ∂U 上的空间曲线)] 为边缘. 这个曲面的面积是

$$F[u]=\int_U\left(1+|\nabla u|^2\right)^{1/2}\mathrm{d}x \tag{7}$$

设有一个函数 u_0 能在所有的具有同样边缘的曲面中把上述面积极小化. 对于这个所谓的极小曲面的几何性态, 能够导出些什么来?

还是如上面那样进行: 写出 $f(t)=F[u_0+tw]$, 对 t 求导等等. 经过一些计算, 最终发现, 在区域 U 内,

$$\operatorname{div}\left(\frac{\nabla u_0}{\left(1+|\nabla u_0|^2\right)^{1/2}}\right)=0, \tag{8}$$

这里的 div 是散度算子. 这个非线性 PDE 就是极小曲面方程, 其左方的表达式结果是 u_0 的图像的平均曲率 (的 2 倍). 所以证明了: 一个极小曲面处处有 0 平均曲率.

在物理上, 有时把极小曲面看成一个肥皂泡, 其边缘张在由 g 的图像所成的框架上.

3.2 推广: 欧拉–拉格朗日方程

现在, 把面积泛函 (7) 代之以一般的表达式

$$F[u]=\int_U L(\nabla u,u,x)\,\mathrm{d}x \tag{9}$$

就是一件直截了当的事情了, 而且有时非常有利, 这里的 U 是 $\mathbf{R}^n$ 的一个区域. 设 u_0 是满足某些附加条件的极小化子, 又能导出欧拉–拉格朗日方程

$$-\operatorname{div}\left(\nabla_v L(\nabla u_0,u_0,x)\right)+L_z(\nabla u_0,u_0,x)=0. \tag{10}$$

它是极小化子必须满足的非线性 PDE. 给定一个 PDE, 如果它具有这个形式, 就称之为一个变分方程.

举一个例子. 如果取 $L(v,z,x)=\frac{1}{2}|v|^2+G(z)$, 相应的欧拉–拉格朗日方程就是非线性泊松方程

$$\Delta u=g(u),$$

其中 $g=G'(z)$, 而 $\Delta u=\sum_{k=1}^{n} u_{x_k x_k}$ 是 u 的拉普拉斯算子[I.3 §5.4]. 我们已经看到了这个重要的 PDE 是一个变分方程. 这是一个很有价值的洞察, 因为这样就可以通过构造泛函 $F[u]=\int_U (|\nabla u|^2/2+G(u))\mathrm{d}x$ 的极小化子 (或其他临界点) 来找到 PDE 的解.

4. 变分法的进一步的问题

前面的例子已经很有说服力地表明了这个很简单的称为计算一阶变分的方法在用于正确的物理和几何问题时是多么有力. 事实上, 变分原理和方法出现在物理和数学二者的好些分支里. 数学家认为是最重要的对象中, 其背后都有某种变分原理. 下面的清单给人以深刻的印象：除了考虑过的例子以外, 这个清单里还有：哈密顿方程、Yang-Mills 方程、Selberg-Witten 方程、各种非线性波方程、统计物理里的吉布斯态和最优控制理论中的动态规划方程.

还留下许多问题. 例如, 如果 $f=f(t)$ 在 t_0 处有一个极小, 则不但有 $(\mathrm{d}f/\mathrm{d}t)(t_0)=0$, 还有 $(\mathrm{d}^2f/\mathrm{d}t^2)(t_0)\geqslant 0$. 专心的读者会正确地猜到, 这一点的推广, 称为二阶变分的计算, 在变分法里面是很重要的. 它使我们洞察到要有适当的凸性条件来保证临界点实际上是稳定的极小化子, 更为基本的是极小化子或其他临界点的存在问题. 数学家们在这里用了极大的智慧来设计适当的函数空间, 使得在其中可以找到 “广义解”(或称“弱解”). 但是这些弱解不一定是光滑的, 所以又必须处理进一步的正规性问题, 以及 (或者) 奇点问题.

但是, 它们都是高度技巧性的数学问题, 超出了本文的范围. 我们的讨论只能结束于此, 并且深切希望对于读者的精力的要求, 已经是极小化的了.

III.95　簇
(Varieties)

圆周和抛物线是簇的两个简单例子. 它们都是用多项式方程来定义的：$x^2+y^2=1$ 和 $y=x^2$. 再加上一个限制, 簇就是一个多项式方程组的解集合. 这里的限制就在于有一些例子我们不想把它们也纳入簇的概念中. 例如, 方程 $x^2-y^2=0$ 的解集合就是两条直线：$x=y$ 和 $x=-y$, 它们自然地分成两片. 所以, 一个多项式方程组的解集称为一个代数集合, 如果它不能写成更小的代数集合的并, 就称为一个簇.

上面给定的例子都是平面 $\mathbf{R}^2$ 的子集合. 但是, 簇这个概念要广泛得多, 簇可以生活在 $\mathbf{R}^n$ 中, 而 n 是任意的; 也可以生活在 $\mathbf{C}^n$ 中, 而 n 也是任意的. 事实上, 对于任意的域 $\mathbf{F}$, 这个定义在 $\mathbf{F}^n$ 中也是有意义的, 而且有趣且重要.

迄今所定义的簇都是仿射簇. 为了许多目的, 处理射影簇更加方便. 定义是类似的, 但是它们生活在射影空间[III.72] 里, 而定义它们所用的多项式必须是齐次的, 即解的任意倍数仍然是解.

更多的信息可以参看条目代数几何[IV.4] 和算术几何[IV.5].

III.96 向 量 丛

(Vector Bundles)

令 X 为一个拓扑空间[III.90]. 粗略地说, 一个向量丛就是对 X 的每一点 x 附加上一个向量空间, 而且使得当 x“连续变动” 时, 这些空间也要连续地变动. 作为一个例子, 考虑 $\mathbf{R}^3$ 中的一个光滑曲面 X. 对于曲面上每一点 x 都有 X 的切平面, 它当然随 x 而连续变动, 而且可以自然地看成一个 2 维向量空间. 下面是准确的定义: X 上的一个秩为 n 的向量丛, 就是一个拓扑空间 E 连同一个连续映射 $p: E \to X$, 使得 X 的每一点 x 的原像 $p^{-1}(x)$(即 E 中被映为 x 的点的集合) 都是一个 n 维向量空间. X 上最显然的秩为 n 的向量丛就是 $\mathbf{R}^n \times X$, 这里的映射规定为 $p(v,x) = x$, 这个向量丛称为平凡丛. 然而, 有趣的丛是非平凡丛, 例如 2 维球面的切平面丛 (即切丛). 从了解一个拓扑空间的向量丛就可以对此拓扑空间懂得很多. 所以, 向量丛在代数拓扑学中处于中心地位, 详见条目代数拓扑[IV.6 §5].

III.97 冯 · 诺依曼代数

(Von Neumann Algebras)

群[I.3 §2.1]G 的酉表示就是一个群的同态[I.3 §4.1], 把 G 的任意元 g 与作用在某个希尔伯特空间[III.37]H 上的酉映射[III.50 §3.1]U_g 连接起来. 一个冯 · 诺依曼代数是一类特殊的 C^*-代数[III.12], 而与酉表示理论有密切的关系. 定义冯 · 诺依曼代数有好几个等价的方法, 下面是其中之一. 可以证明, 给定了一个酉表示, 定义其换位子 (commutant) 为所有与此酉表示中一切 U_g 都可以交换的 $B(H)$ 的算子[III.50] 的集合. 这些算子构成一个 C^*-代数, 而冯 · 诺依曼代数就是这样产生的. 它们也可以抽象地定义如下: 一个 C^*-代数 A 是一个冯 · 诺依曼代数, 如果存在一个巴拿赫空间[III.62] X, 使得 X 的对偶[III.19 §4] 就是 A(A 本身也看成是一个巴拿赫空间).

冯 · 诺依曼代数的建筑要素是一类特殊的称为因子 (factor) 的冯 · 诺依曼代数. 主要的研究课题就是因子的分类, 其中包括一些 20 世纪后半世纪最著名的定理, 更多的知识可以参看条目算子代数[IV.15 §2].

III.98 小　波

(Wavelets)

如果想把一张黑白照片从一个计算机发送到另一个计算机上去, 做这件事情的一个明显的方法是按像素把这张照片编码: 见到黑色的像素就编码为 0, 而白色像素编码为 1. 然而, 对于某些照片, 这个方法显然是极为低效率的. 例如, 设这张照片是正方形的, 左半全是白的, 而右半全是黑的, 那么传送几条指令来重构这幅图片要比列出每一个像素好得多. 进一步说, 这些像素的精确的信息通常不起作用, 如果想要插入一点灰色, 那么只需要规定黑色和白色像素有一定的比, 而且保证这两种像素都均匀分布就行了.

然而, 找出对图片编码的好方法是很困难的, 是工程中的一个重要研究领域. 但是一张图片可以看作是一个从一个矩形到 $\mathbf{R}$ 的函数. 所有这些函数的集合是一个向量空间[I.3 §2.3], 而找出一个好的编码的自然的方法是找出这个空间的好的基底. 这里所谓“好”就是指我们感兴趣的函数 (就是相应于要想传送的那一类图形表示的函数) 只要少数几个系数就可以决定了. 当然这里会有些微小的变化, 但是又是人眼难以觉察的.

对于许多的目的, 小波是特别好的基底. 它们在某些方面很像傅里叶变换[III.27], 但是在对一些细节的编码上要好得多, 例如对鲜明的轮廓线, 以及对那些“局部化”的而不是弥散到整个图形的那些图案或花样, 更多细节请参看条目小波及其应用[VII.3].

III.99　策墨罗–弗朗克尔公理

(The Zermelo-Fraenkel Axioms)

策墨罗–弗朗克尔公理 (以下简记为 ZF 公理) 是一组作为集合论基础的公理, 可以从两个角度来看它. 第一是把它看成允许在集合上施行的一组“可容许运算”, 例如其中有一条公理指出, 任意给定两个集合 x 和 y, 一定存在一个“对子集合”(pair set), 其元素就只是 x 和 y.

ZF 公理之所以重要的理由之一是: 可以把整个数学都归结为集合论, 这样, ZF 公理就可以看成是整个数学的基础. 当然, ZF 公理想要做到这一点, 至关重要的就是, ZF 公理所容许的运算要使得我们可以作所有通常的数学运算. 结果就使得有些公理非常微妙.

看待 ZF 公理的另一种角度是: ZF 公理正是我们想要从空集开始把集合的整

个宇宙都 “建造” 起来所需要的公理. 我们可以细看 ZF 公理的每一条公理, 看看它在我们建造集合的宇宙时所起的本质的作用. 等价地说, 它们是一些 “封闭性规则”, 使得集合的任何的宇宙, 或者准确一些说, 使得集合理论的任意模型都必须服从. 这样, 例如其中有一条公理指出, 每一个集合都有幂集合 (即所有子集合的集合), 而这个公理就使得我们能够从空集合开始, 做出为数巨大的集合来: 可以得到空集合的幂集合、空集合的幂集合的幂集合, 如此等等. 说真的, 所有集合的宇宙 (在一定意义下) 就是空集合在 ZF 公理所容许的运算下的闭包.

ZF 公理是用一阶逻辑[IV.23 §1] 写出来的. 所以, 每一条公理中都可以提到变元 (可以解释为遍取所有的集合) 和通常的逻辑运算, 还有一个 “原始的关系” 即属于关系. 例如, 对子集合公理就可以形式地写为

$$(\forall x)\,(\forall y)\,(\exists z)\,(\forall t)\,(t \in z \Leftrightarrow t = x \text{ or } t = y)\,.$$

按照规约, ZF 公理中不包括选择公理[III.1]. 如果把选择公理也包括进来, 这样的公理系统就称为 ZFC 公理.

关于 ZF 公理的进一步的讨论, 请参看条目集合理论[IV.22 §3.1].